A Variant of the VC-Dimension with Applications to Depth-3 Circuits

Peter Frankl
Rényi Institute, Budapest, Hungary

Svyatoslav Gryaznov
Institute of Mathematics of the Czech Academy of Sciences, Prague, Czech Republic
St. Petersburg Department of V.A. Steklov Institute of Mathematics of the Russian Academy of Sciences, Russia

Navid Talebanfard
Institute of Mathematics of the Czech Academy of Sciences, Prague, Czech Republic

Abstract

We introduce the following variant of the VC-dimension. Given $S \subseteq \{0,1\}^n$ and a positive integer d, we define $\mathbb{U}_d(S)$ to be the size of the largest subset $I \subseteq [n]$ such that the projection of S on every subset of I of size d is the d-dimensional cube. We show that determining the largest cardinality of a set with a given $\mathbb{U}_d$ dimension is equivalent to a Turán-type problem related to the total number of cliques in a d-uniform hypergraph. This allows us to beat the Sauer–Shelah lemma for this notion of dimension. We use this to obtain several results on Σ_3^k-circuits, i.e., depth-3 circuits with top gate OR and bottom fan-in at most k:

- Tight relationship between the number of satisfying assignments of a 2-CNF and the dimension of the largest projection accepted by it, thus improving Paturi, Saks, and Zane (Comput. Complex. '00).
- Improved Σ_3^3-circuit lower bounds for affine dispersers for sublinear dimension. Moreover, we pose a purely hypergraph-theoretic conjecture under which we get further improvement.
- We make progress towards settling the Σ_3^2 complexity of the inner product function and all degree-2 polynomials over $\mathbb{F}_2$ in general. The question of determining the Σ_3^3 complexity of IP was recently posed by Golovnev, Kulikov, and Williams (ITCS'21).

2012 ACM Subject Classification Theory of computation → Circuit complexity; Mathematics of computing → Combinatoric problems; Mathematics of computing → Hypergraphs

Keywords and phrases VC-dimension, Hypergraph, Clique, Affine Disperser, Circuit

Digital Object Identifier 10.4230/LIPIcs.ITCS.2022.72

Related Version *Full Version*: `https://arxiv.org/abs/2111.09671`

Funding *Svyatoslav Gryaznov*: Supported by GAČR grant 19-05497S. The Institute of Mathematics of the Czech Academy of Sciences is supported by RVO: 67985840.
Navid Talebanfard: Supported by GAČR grant 19-27871X.

Acknowledgements We are grateful to Vojtěch Rödl for discussions and to ITCS'22 reviewers for useful comments.

1 Introduction

Boolean circuits provide a natural model for computing Boolean functions. Given a Boolean function f in variables $x_1, \dots, x_n$, a circuit is a sequence $C = \langle g_1, \dots, g_t \rangle$ of functions where each g_i is either an input variable, its negation, or $g_i = g(g_{i_1}, g_{i_2})$ where $i_1, i_2 < i$ and g is an arbitrary Boolean function. The output of the circuit on an input x is given by the last function, that is, $C(x) = g_t(x)$. The size of the circuit C is t, the length of the sequence. A well-known simple counting argument due to Shannon shows that almost all Boolean

13th Innovations in Theoretical Computer Science Conference (ITCS 2022).
Editor: Mark Braverman; Article No. 72; pp. 72:1–72:19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

functions in n variables require circuits of size $2^n/n$ (see [17] for a proof and more background on circuit complexity). Despite this fact, the best known circuit size lower bound for an explicit function is barely above $3n$ [10]. It is known that the arguments used in this result, the so-called gate elimination technique, cannot even yield a lower bound of $5n$ [14]. Thus, a super-linear size lower bound even for logarithmic depth circuits would make a breakthrough in the formidable wall of complexity theory.

1.1 Valiant's program and depth-3 circuits

Another natural model of computation is bounded-depth circuits with unbounded fan-in. Let Σ_3^k denote the class of depth-3 circuits of the form $\mathrm{OR} \circ \mathrm{AND} \circ \mathrm{OR}$ with bottom fan-in at most k. Equivalently we can view a Σ_3^k-circuit as an unbounded disjunction of k-CNF formulas. Valiant [31] formulated a program to prove super-linear lower bounds for $O(\log n)$-depth circuits. He showed that a lower bound of $2^{\omega(n/\log\log n)}$ for $\Sigma_3^{n^\epsilon}$ circuits for some $\epsilon > 0$ implies a super-linear lower bound for $O(\log n)$-depth fan-in 2 circuits. Furthermore, he showed that if we restrict the depth-3 circuits to $\Sigma_3^{O(1)}$ then a lower bound larger than $2^{n/2}$ implies a super-linear lower bound for series-parallel circuits. This gives a strong motivation to prove Σ_3^k-circuit lower bounds for a fixed function for every constant k. In this direction Paturi, Pudlák, and Zane [23] proved a lower bound of $\Omega(2^{n/k})$ for the parity function. Later Paturi, Pudlák, Saks, and Zane [22] using similar but stronger techniques gave a lower bound of $\Omega(2^{n\pi^2/6k})$ for the characteristic function of the BCH code. This remains the best known result of this type.

Recently Golovnev, Kulikov, and Williams [15] in an insightful revisiting of Valiant's program showed among other things that a lower bound of $2^{n-o(n)}$ for Σ_3^{16}-circuits implies a $3.9n - o(n)$ size lower bound for unrestricted circuits. This is a significant result since as we mentioned earlier the best lower bounds for unrestricted circuits are much weaker. This gives a strong motivation to study Σ_3^k-circuits for small values of k, and in fact, a result in this direction is known. Paturi, Saks, and Zane [24] proved a $2^{n-o(n)}$ lower bound for $k = 2$. For $k \geq 3$ no such bounds are known.

Lower bound arguments. Let us briefly recall the general strategy in Σ_3^k-circuit lower bounds. Let f be our hard function. If we can show that any k-CNF formula F which is consistent with f, that is $F(x) \leq f(x)$ for all x, has at most R satisfying assignments, then it follows that f requires Σ_3^k-circuits of size at least $\left|f^{-1}(1)\right|/R$. This is because a Σ_3^k-circuit computing f gives a covering of $f^{-1}(1)$ using the sets of satisfying assignments of k-CNF formulas which are consistent with f.

The specific execution of this argument for Σ_3^2 is as follows. Given a CNF formula ϕ, we denote by $\mathrm{sat}(\phi)$ the set of satisfying assignments of ϕ. [24] showed that if $S = \mathrm{sat}(\phi)$ for a 2-CNF formula ϕ in n variables and $|S| = 2^{\Omega(n)}$, then S contains a *projection* of dimension $\Omega(n)$. A projection is simply an affine space defined by equations of the form $x = 0$, $x = 1$, $x = y$ or $x = 1 - y$. Thus, if we have a function f such that $f^{-1}(1)$ has size at least $2^{n-o(n)}$ and does not contain any projection of linear dimension, then f requires Σ_3^2-circuits of size $2^{n-o(n)}$. It turns out that explicit constructions of even more general such functions exist. These are called *affine dispersers* for sublinear dimension, functions which are not constant under any affine space of some $o(n)$ dimension (see, e.g., [3])[1]. One may ask if it is possible to

[1] Note that these functions were explicitly constructed more than a decade after [24] appeared. That paper got around this by constructing a disperser from a pseudo-random distribution.

extend the above result regarding projections to k-CNFs for $k \geq 3$ and thus obtain Σ_3^k lower bounds. However, [24] showed that there are 4-CNFs with exponentially many satisfying assignments which have only projections of constant dimension (later we will show that there are even 3-CNFs with this property). This limits the applicability of projections to k-CNFs for $k \geq 3$, but it is conceivable that every sufficiently large set of satisfying assignments of a k-CNF contains a large *general* affine subspace.

Affine dispersers. Given $S \subseteq \{0,1\}^n$ let $\mathbb{AF}(S)$ denote the dimension of the largest affine space contained in S. Given c define

$$\mathrm{af}_k(c) := \inf_n \min \{\mathbb{AF}(\mathrm{sat}(\phi))/n : \phi \text{ is } k\text{-CNF in } n \text{ variables, } |\mathrm{sat}(\phi)| \geq 2^{cn}\}.$$

Note that $\mathrm{af}_k(0) = 0$ and $\mathrm{af}_k(1) = 1$. For every k define c_k to be the infimum of c for which $\mathrm{af}_k(c) > 0$. Observe that an affine disperser for sublinear dimension requires Σ_3^k-circuits of size $2^{(1-c_k)n-o(n)}$ (we may assume that our function has $2^{n-o(n)}$ ones, otherwise the negation of the function, which is also an affine disperser, does). In particular, if $c_k = 0$ for every k then we get superlinear lower bounds for series-parallel circuits, and if $c_{16} = 0$ then affine dispersers require general circuits of size $3.9n - o(n)$. Interestingly the state-of-the-art general circuit lower bounds are proved for such affine dispersers [10]. Thus finding upper bounds on c_k is a justified direction to explore. So far we know only that $c_2 = 0$ [24]. For arbitrary k the best upper bound to our knowledge can be easily inferred from the Switching Lemma (see [21, 25]): any k-CNF in n variables has a decision tree representation of size $2^{(1-1/Ck)n}$, where $C > 1$ is a universal constant, and thus a k-CNF that accepts significantly more than $2^{(1-1/Ck)n}$ assignments, in particular, accepts a large subcube, which is the simplest form of an affine space. The constant C comes from the constant appearing in the Switching Lemma which can be set to 10. It follows that $c_k \leq 1 - \frac{1}{10k}$.

1.2 Our contributions

We introduce a variant of the VC-dimension which allows better Sauer–Shelah type lemmas [27, 28]. Recall that for a set $S \subseteq \{0,1\}^n$ the VC-dimension of S, $\mathbb{VC}(S)$, is defined to be the size of the largest subset $I \subseteq [n]$ such that S projected on coordinates in I is the $|I|$-dimensional cube. This is a fundamental concept from learning theory [32] which is also extensively studied in combinatorics (see, e.g., [5, 4, 2]). It is also used in circuit complexity (see, e.g., [24, 16] for depth-3, and [9, 20] for general circuits). Applications of the VC-dimension usually go through the Sauer–Shelah lemma which states that if $|S| > \sum_{i=0}^{r} \binom{n}{i}$ then $\mathbb{VC}(S) \geq r + 1$. This bound is tight and it is sufficient for most applications since it implies that if $|S| \geq 2^{\Omega(n)}$ then $\mathbb{VC}(S) \geq \Omega(n)$. However, this bound cannot guarantee the VC-dimension to be bigger than $n/2$ for sets of size $2^{\Omega(n)}$. To see this consider the set of all n-bit strings with Hamming weight at most $n/2$. This set has size 2^{n-1} but VC-dimension only $n/2$.

A variant of the VC-dimension. The variant we consider is very natural. Given a set $S \subseteq \{0,1\}^n$ and a positive integer d, $\mathbb{U}_d(S)$ is the size of the largest subset $I \subseteq [n]$ such that the projection of S to every subset of I of size d is the d-dimensional cube. We show that the size of the largest set $S \subseteq \{0,1\}^n$ with $\mathbb{U}_d(S) = r$ is the same as the maximum number of cliques in an n-vertex d-uniform hypergraph with no clique of size $r + 1$. Luckily for $d = 2$ this quantity can be computed exactly from a generalization of Turán's theorem due to Zykov, and it turns out to be $\left(\frac{n}{r} + 1\right)^r$. Note that this immediately overcomes the $n/2$ barrier of the VC-dimension mentioned before: for the above example we have $\mathbb{U}_{n/2}$ dimension exactly n

and in general for every $\epsilon > 0$ there exists $\delta < 1$ such that if $|S| > 2^{\delta n}$ then $\mathbb{U}_2(S) \geq (1-\epsilon)n$. For larger values of d we can determine this bound when $r \geq (1-1/d)n$. For other values, we state a conjecture that extends Zykov's theorem to d-uniform hypergraphs.

Applications. We obtain several results regarding depth-3 circuits.

- Bottom fan-in 2: The first application is a tightening of [24] relating the dimension of the largest projection contained in the set of satisfying assignments of a 2-CNF and its size. This allows us to obtain the following results.
  - *Lower bounds for weaker affine dispersers:* We prove lower bounds on the size of Σ_3^2 circuits for affine dispersers for linear dimension. This is interesting since [24] does not give anything for affine dispersers for dimension bigger than $n/2$.
  - *Progress on the complexity of the inner product function (IP):* The general strategy for proving Σ_3^k circuit lower bounds described above does not give optimal bounds for some functions, notably the inner product function IP. [15] also poses the question of proving tight bottom fan-in 3 lower bounds for IP. But tight lower bounds are not known even for bottom fan-in 2 and here we focus on this case. We show that any 2-CNF consistent with the IP on n variables accepts at most $3^{n/2}$ assignments and this is tight. Thus, we obtain a Σ_3^2-circuit size lower bound of $2^{0.20n}$ that is worse than the best known $2^{0.25n}$ lower bound, which follows from a reduction to parity. However, we show that there is a unique 2-CNF consistent with IP achieving this bound. This suggests that an alternative approach to lower bounds, namely the stability approach, might be fruitful. Stability results show that a large set avoiding a certain forbidden structure looks very similar to the unique extremal set (see, e.g., [18, 12]). In circuit complexity we are only aware of one such result, which can be found in a work of Dinur and Meir [8]. Perhaps it is possible to show that a 2-CNF consistent with IP which has many satisfying assignments has a particular structure, and this might allow us to prove the desired lower bound.
  - *Complexity of degree-2 polynomials over $\mathbb{F}_2$:* We show that any such polynomial in n variables requires Σ_3^2-circuits of size $2^{n/10}$. Impagliazzo, Paturi, and Zane [16] showed that almost all degree-2 polynomials require Σ_3^k-circuits of size $2^{n-o(n)}$ for $k = O(1)$. Thus developing lower bound arguments for these functions contributes to the program of finding explicit hard degree-2 polynomials. The complexity of these functions has been studied previously for depth-3 circuits with XOR at bottom by Cohen and Shinkar [7].
- Bottom fan-in 3: Assuming that a 3-CNF has sufficiently many satisfying assignments we give a large projection contained in the set of satisfying assignments which also yields a Σ_3^3 lower bound for affine dispersers. This follows from our lower bound on $\mathbb{U}_3$ for sufficiently large sets. In particular, it implies that $c_3 \leq \frac{\log 7}{3} \simeq 0.936$. Note that this is less than the $\frac{29}{30} \simeq 0.966$ bound which follows from the Switching Lemma. Although this improvement is modest, the underlying conceptual arguments seem to provide new insight. Our technique poses a Turán-type conjecture for hypergraphs which, if true, would imply $c_3 \leq 0.707$.

2 The $\mathbb{U}_d$ dimension

▶ **Definition 1.** *Let $\mathcal{F} \subseteq 2^{[n]}$ be a set system and let $I \subseteq [n]$. The* trace *of $\mathcal{F}$ on I is defined by $\mathrm{Tr}_{\mathcal{F}}(I) := \{A \cap I : A \in \mathcal{F}\}$. Equivalently, viewing $\mathcal{F}$ as a subset of $\{0,1\}^n$, $\mathrm{Tr}_{\mathcal{F}}(I)$ is the set of distinct vectors obtained by projecting $\mathcal{F}$ on the coordinates in I.*

▶ **Definition 2.** *Let $\mathcal{F} \subseteq 2^{[n]}$ be a set system. We say that $I \subseteq [n]$ is* shattered *if $|\mathrm{Tr}_{\mathcal{F}}(I)| = 2^{|I|}$. Given $\mathcal{F}$ the VC-dimension of $\mathcal{F}$, denoted by $\mathbb{VC}(\mathcal{F})$, is the size of the largest shattered set.*

▶ **Definition 3** (d-Universality)**.** *Let $\mathcal{F} \subseteq 2^{[n]}$ be a set system and d a positive integer. We say that $I \subseteq [n]$ is* d-universal *for $\mathcal{F}$ if $|I| \geq d$ and every $J \subseteq I$ with $|J| = d$ is shattered. We say that $\mathcal{F}$ has* property $U(r, d)$ *if there exists $I \subseteq [n]$ of size r which is d-universal. We denote by $u(n, r, d)$ the cardinality of the largest system of subsets of $[n]$ which does not have property $U(r+1, d)$. We write $\mathbb{U}_d(\mathcal{F})$ to denote the size of the largest d-universal set for $\mathcal{F}$.*

It immediately follows from the definition that if $\mathbb{VC}(\mathcal{F}) \geq d$ then $\mathbb{U}_d(\mathcal{F}) \geq \mathbb{VC}(\mathcal{F})$. To prove an upper bound on $u(n, r, d)$ we observe that it is sufficient to consider downward closed systems. We adopt the squashing argument of Frankl [11].

▶ **Lemma 4.** *Let $\mathcal{F} \subseteq 2^{[n]}$ be a set system not having property $U(r+1, d)$ such that $\sum_{A \in \mathcal{F}} |A|$ is minimized over all such families of cardinality $|\mathcal{F}|$. Then $\mathcal{F}$ is a downward closed family.*

Proof. Assume for a contradiction that $\mathcal{F}$ is not downward closed. Then there exists $A \in \mathcal{F}$ and $i \in [n]$ such that $A \setminus \{i\} \notin \mathcal{F}$. For any $B \subseteq [n]$ we define

$$B' := \begin{cases} B \setminus \{i\} & \text{if } i \in B \text{ and } B \setminus \{i\} \notin \mathcal{F} \\ B & \text{otherwise.} \end{cases}$$

We now define $\mathcal{F}' := \{B' : B \in \mathcal{F}\}$. Note that $\left|\mathcal{F}'\right| = |\mathcal{F}|$ and since $A' = A \setminus \{i\}$, $\sum_{C \in \mathcal{F}'} |C| < \sum_{D \in \mathcal{F}} |D|$. Therefore, by the minimality assumption, $\mathcal{F}'$ has property $U(r+1, d)$ and hence there exists $I \subseteq [n]$ with $|I| = r + 1$, which is d-universal for $\mathcal{F}'$. We will show that I is d-universal also for $\mathcal{F}$, which is a contradiction. Since $\mathcal{F}$ and $\mathcal{F}'$ agree on all elements except for i, we may assume that $i \in I$. By the same reasoning $I \setminus \{i\}$ is d-universal for $\mathcal{F}$. Therefore, it remains to show that for any $J \subseteq I \setminus \{i\}$ with $|J| = d - 1$, $|\mathrm{Tr}_{\mathcal{F}}(J \cup \{i\})| = 2^d$. We will show that for any $S \subseteq J$, we have that both S and $S \cup \{i\}$ are in $\mathrm{Tr}_{\mathcal{F}}(J \cup \{i\})$. By d-universality $S \cup \{i\} \in \mathrm{Tr}_{\mathcal{F}'}(J \cup \{i\})$ and hence there exists $E \in \mathcal{F}'$ such that $S \cup \{i\} = E \cap (J \cup \{i\})$. Since $i \in E$, by construction of $\mathcal{F}'$, it follows that $E \in \mathcal{F}$ and hence $S \cup \{i\} \in \mathrm{Tr}_{\mathcal{F}}(J \cup \{i\})$. Furthermore, again since $i \in E$ and by construction of $\mathcal{F}'$, $E \setminus \{i\} \in \mathcal{F}$. Since $S = (E \setminus \{i\}) \cap (J \cup \{i\})$, we have $S \in \mathrm{Tr}_{\mathcal{F}}(J \cup \{i\})$. ◀

Given a d-uniform hypergraph (or a d-graph) $H = (V, E)$, a clique $S \subseteq V$ is a subset of vertices such that either $|S| < d$ or if $|S| \geq d$ then any subset of S of size d is a hyperedge in E. Analogously, S is an independent set if it does not contain any hyperedge. We denote the d-uniform clique of size t by K_t^d. Let us denote by $k(n, r, d)$ the maximum number of cliques in a K_{r+1}^d-free d-graph on n vertices.

▶ **Lemma 5.** *For every $n \geq r \geq d$, $u(n, r, d) = k(n, r, d)$.*

Proof. To show the lower bound, let $H = ([n], E)$ be a K_{r+1}^d-free d-graph achieving the maximum number of cliques. We define

$$\mathcal{F} := \{S \subseteq [n] : S \text{ is a clique in } H\}.$$

Note that by construction $\mathcal{F}$ is downward closed. Assume for a contradiction that there exists $I \subseteq [n]$ of size $r + 1$ which is d-universal for $\mathcal{F}$. By d-universality and downward closedness, every subset of I of size d is in $\mathcal{F}$ which implies that I is a clique in H.

In the other direction let $\mathcal{F}$ be a system of maximum size not having property $U(r+1,d)$. By Lemma 4 we may assume that $\mathcal{F}$ is downward closed. We define a d-graph $H=([n],E)$ as follows:

$$E \coloneqq \{S \in \mathcal{F} : |S| = d\}.$$

Since $\mathcal{F}$ is downward closed, any clique $S \subseteq [n]$ is d-universal for $\mathcal{F}$. Therefore, H is K^d_{r+1}-free. Note furthermore that each $S \in \mathcal{F}$ gives a clique in H. Thus, the size of $\mathcal{F}$ is bounded by the total number of cliques in H. ◀

Using Lemma 5 and a generalization of Turán's Theorem, which has been rediscovered many times, we can determine $u(n,r,2)$ precisely. Recall that the *Turán graph* $T_{n,r}$ is the complete n-vertex r-partite graph with parts of sizes as equal as possible.

▶ **Theorem 6** (Zykov [33], Sauer [26], Alekseev [1])**.** *Let G be a K_{r+1}-free graph on n vertices. Then $k(G) \le k(T_{n,r}) \le (\frac{n}{r}+1)^r$.*

Applying Lemma 5 and Theorem 6 immediately implies the following.

▶ **Theorem 7.** *For every $n \ge r$, $u(n,r,2) = k(T_{n,r}) \le (\frac{n}{r}+1)^r$. It follows that for every $\mathcal{F} \subseteq 2^{[n]}$, $|\mathcal{F}| \le (\frac{n}{\mathbb{U}_2(\mathcal{F})}+1)^{\mathbb{U}_2(\mathcal{F})}$.*

We now determine $u(n,r,d)$ when r is sufficiently large. Note that by complementation $k(n,r,d)$ is the same as the maximum number of independent sets in an n-vertex d-graph with no independent set of size $r+1$. Given a hypergraph $H=(V,E)$, a transversal $T \subseteq V$ is a subset of vertices such that every edge of H contains at least one vertex from T. Denote by $i(n,r,d)$ the maximum number of independent sets in an n-vertex d-graph with no transversal of size $r-1$. It is easy to see that

$$i(n,r,d) = k(n,n-r,d) \tag{1}$$

since an n-vertex d-graph has no transversal of size $r-1$ if and only if it does not have any independent set of size $n-r+1$.

▶ **Theorem 8.** *Let $r \le n/d$ and let $H=(V,E)$ be a d-graph on n vertices with no transversal of size $r-1$ and maximum possible number of independent sets. Then H is the disjoint union of r hyperedges and $n-rd$ isolated vertices. Consequently, $i(n,r,d) = 2^{n-rd}(2^d-1)^r$.*

To prove this theorem we need the following auxiliary lemma.

▶ **Lemma 9.** *Let X be a set of size d. Consider a distribution μ on the subsets of X with the following properties:*

1. *$\mu(X) = 0$.*
2. *$\mu(F) \ge \mu(F')$ if $F \subseteq F'$.*

Then

$$\mathop{\mathbb{E}}_{F\sim\mu}\left[|\overline{F}|\right] \ge d\frac{2^{d-1}}{2^d-1}.$$

The equality holds if and only if $\mu(F) = \frac{1}{2^d-1}$ for every $F \subsetneq X$. In other words, $\mathop{\mathbb{E}}_{F\sim\mu}\left[|\overline{F}|\right]$ is minimized if μ is the uniform distribution over all non-full sets.

Proof. Let us denote by $[X]^i$ the set of subsets of X of size i. Define ν on $\{0, 1, \dots, d\}$ as follows:

$$\nu(i) := \frac{\sum\limits_{F \in [X]^i} \mu(F)}{\binom{d}{i}}.$$

▷ Claim 10. For every i, $\nu(i) \geq \nu(i+1)$. The equality holds if and only if $\mu(F) = \mu(F')$ for every $F \subseteq F' \subsetneq X$, where $|F| = i$ and $|F'| = i + 1$.

Proof. We need to show that

$$\frac{\sum\limits_{F \in [X]^i} \mu(F)}{\binom{d}{i}} \geq \frac{\sum\limits_{F \in [X]^{i+1}} \mu(F)}{\binom{d}{i+1}},$$

which is equivalent to

$$(d - i) \sum_{F \in [X]^i} \mu(F) \geq (i + 1) \sum_{F \in [X]^{i+1}} \mu(F). \tag{2}$$

Consider the sum

$$\sum_{\substack{(F,F'),\text{ where } F \subseteq F',\\ F \in [X]^i, F' \in [X]^{i+1}}} \mu(F).$$

Each $\mu(F)$, where $|F| = i$, appears exactly $d - i$ times since there are $d - i$ choices of F' such that $F \subseteq F'$ and $|F'| = i + 1$. Thus, it is equal to

$$\sum_{F \in [X]^i} (d - i)\mu(F). \tag{3}$$

Similarly,

$$\sum_{\substack{(F,F'),\text{ where } F \subseteq F',\\ F \in [X]^i, F' \in [X]^{i+1}}} \mu(F') = \sum_{F' \in [X]^{i+1}} (i + 1)\mu(F'). \tag{4}$$

By the second property of μ, (3) is at least (4), which gives us (2).

For the second part note that equality in (2) holds if and only if $\mu(F) = \mu(F')$, where $F \subseteq F'$, $F \in [X]^i$, and $F' \in [X]^{i+1}$. ◁

By definition of ν,

$$\mathop{\mathbb{E}}_{F \sim \mu} \left[|\overline{F}|\right] = \sum_{F \subseteq X} (d - |F|)\mu(F) = \sum_{i=0}^{d} (d - i)\binom{d}{i}\nu(i).$$

We can rewrite the last sum as

$$\sum_{j=0}^{d-1} \sum_{i=0}^{j} \binom{d}{i}\nu(i). \tag{5}$$

We need the following simple fact.

▶ **Lemma 11.** *Let $\{a_i\}_{i=1}^n$ be a sequence of non-decreasing numbers $a_1 \geq a_2 \geq \ldots \geq a_n$. Let $\{b_i\}_{i=1}^n$ be a sequence of non-negative numbers with $\sum\limits_{i=1}^{n} b_i > 0$. Then for every $1 \leq m \leq n$*

$$\sum_{i=1}^{m} a_i b_i \geq \frac{\sum\limits_{i=1}^{m} b_i}{\sum\limits_{i=1}^{n} b_i} \sum_{i=1}^{n} a_i b_i.$$

Proof. Define a random variable X on $[n]$ which takes value i with probability

$$\frac{b_i}{\sum\limits_{j=1}^{n} b_j}.$$

Observe that

$$\mathbb{E}[a_X] = \frac{1}{\sum\limits_{i=1}^{n} b_i} \sum_{i=1}^{n} a_i b_i,$$

and

$$\mathbb{E}[a_X | X \leq m] = \frac{1}{\sum\limits_{i=1}^{m} b_i} \sum_{i=1}^{m} a_i b_i.$$

Using a simple coupling argument we show that $\mathbb{E}\left[a_X \mid X \leq m\right] \geq \mathbb{E}[a_X]$ which gives the result. We jointly sample (A, B) such that A is distributed as X and B is distributed as X conditioned on $X \leq m$. Furthermore, we guarantee that $B \geq A$ which by the assumption that $a_1 \geq \ldots \geq a_n$ implies $a_B \geq a_A$.

We first sample A. If $A \leq m$ then we set $B = A$. Otherwise, we sample B as X conditioned on $X \leq m$. It is easy to see that (A, B) satisfies our requirements. ◀

Since μ is a distribution and $\mu(X) = 0$, we have

$$\sum_{i=0}^{d-1} \binom{d}{i} \nu(i) = \sum_{F \subsetneq X} \mu(F) = 1. \tag{6}$$

From Claim 10, Lemma 11 (for $a_i = \nu(i)$ and $b_i = \binom{d}{i}$), and (6) it follows that for every $0 \leq j \leq d-1$

$$\sum_{i=0}^{j} \binom{d}{i} \nu(i) \geq \frac{\sum\limits_{i=0}^{j} \binom{d}{i}}{2^d - 1}. \tag{7}$$

Hence, we have the following lower bound on (5):

$$\sum_{j=0}^{d-1} \sum_{i=0}^{j} \binom{d}{i} \nu(i) \geq \frac{\sum\limits_{j=0}^{d-1} \sum\limits_{i=0}^{j} \binom{d}{i}}{2^d - 1} = \frac{\sum\limits_{i=0}^{d} (d-i) \binom{d}{i}}{2^d - 1} = d \frac{2^{d-1}}{2^d - 1}. \tag{8}$$

Observe that (8) is an equality if and only if for every $0 \leq j \leq d-1$ (7) is an equality. Equivalently, for every i we have $\nu(i) = \frac{1}{2^d - 1}$. It follows from the second part of Claim 10 that $\mu(F) = \mu(F')$ for every $F \subseteq F' \subsetneq e$. In particular, for every $F \subsetneq e$ we have $\mu(F) = \mu(\varnothing) = \nu(0) = \frac{1}{2^d - 1}$. ◀

This lemma can be used to prove the following result about the number of independent sets in a d-graph. Let us denote by $i(H)$ the number of independent sets in a hypergraph H.

▶ **Lemma 12.** *Let $e = \{u_1, \dots, u_d\}$ be an edge of a d-graph H. Then there exists $u \in e$ such that*

$$i(H) \le \frac{2^d - 1}{2^{d-1}} i(H \setminus u).$$

The equality holds if and only if every no other edge in H intersects e.

Proof. We partition the independent sets in H by their "footprint" on e:

$$\mathcal{I}_F \coloneqq \{I : I \text{ is an independent set of } H, I \cap e = F\}\,, \quad \text{where } F \subseteq e.$$

Since removing any subset of vertices from an independent set leaves it independent, $|\mathcal{I}_F| \ge |\mathcal{I}_{F'}|$ if $F \subseteq F'$. Also, $\mathcal{I}_e = \varnothing$ since e is an edge.

For $u \in e$, we can express the number of independent sets in the hypergraph $H \setminus u$ in terms of $\mathcal{I}_F$.

$$i(H \setminus u) = \sum_{F \subseteq e \setminus \{u\}} |\mathcal{I}_F|\,.$$

Thus, we have the following:

$$\sum_{u \in e} i(H \setminus u) = \sum_{F \subseteq e} (d - |F|)\, |\mathcal{I}_F|\,. \tag{9}$$

Consider a distribution μ defined on the subsets of e as follows:

$$\mu(F) \coloneqq \frac{|\mathcal{I}_F|}{i(H)}.$$

Clearly, μ satisfies all the conditions of Lemma 9. Hence,

$$\sum_{F \subseteq e} (d - |F|)\, |\mathcal{I}_F| \ge d \frac{2^{d-1}}{2^d - 1} i(H). \tag{10}$$

Applying (10) to (9) gives

$$d \frac{2^{d-1}}{2^d - 1} i(H) \le \sum_{u \in e} i(H \setminus u) \le d \max_{u \in e} i(H \setminus u).$$

This concludes the proof of the first part of the statement.

For the second part Lemma 9 also implies that (10) is an equality if and only if $\mu(F) = \frac{1}{2^d - 1}$ for every $F \subsetneq e$. Consequently,

$$|\mathcal{I}_F| = |\mathcal{I}_\varnothing|\,. \tag{11}$$

For every $F \subsetneq e$, consider an injective function $b_F \colon \mathcal{I}_F \to \mathcal{I}_\varnothing$ defined as follows:

$$b_F(I) \coloneqq I \setminus F.$$

It follows from (11) that b_F is a bijection.

Assume that there exists another edge e' such that $F = e \cap e' \ne \varnothing$. $I = e' \setminus F$ is an independent set (its size is smaller than d), and, since b_F is a bijection, $I \cup F = e'$ must be an independent set, which is a contradiction. ◀

Now we can finally prove Theorem 8.

Proof of Theorem 8. We prove it by induction on n and r. For the case $r = 1$, H must be non-empty. Since removing an edge increases the number of independent sets, we can remove all but one edges from H. The hypergraph with exactly one edge has $2^{n-d}(2^d - 1)$ independent sets.

For the inductive step, we use the bound from Lemma 12. Let us denote by $\tau(H)$ the size of a transversal of minimum size in H. Let u be a vertex of H such that u is contained in at least one edge of H. If after removing u the transversal number does not drop, we can remove every edge incident to u, and the resulting graph would not have a transversal of size $r - 1$, but would have more independent sets than H. Thus, without loss of generality, we can assume that for every non-isolated vertex u, $\tau(H \setminus u) = \tau(H) - 1$.

Clearly, H consists of at least one edge. Let e be an edge of H. Lemma 12 together with the induction hypothesis imply that

$$i(H) \leq \frac{2^d - 1}{2^{d-1}} i(H \setminus u) \leq \frac{2^d - 1}{2^{d-1}} 2^{(n-1)-(r-1)d} (2^d - 1)^{r-1} = 2^{n-rd} (2^d - 1)^r,$$

and we have an equality here only if e does not intersect any other edge in H. ◀

The next theorem follows immediately from Theorem 8 and (1).

▶ **Theorem 13.** *Let $r \geq (1 - \frac{1}{d})n$. Then $u(n, r, d) = 2^{n-(n-r)d}(2^d - 1)^{n-r}$.*

In our applications we only use the upper bound on u. We conjecture that the natural extension of Theorem 6 to d-graphs holds. Recall the definition of binomial coefficients to real numbers. Given a positive real x and an integer k with $x \geq k$ we define $\binom{x}{k} := \frac{x(x-1)\dots(x-k+1)}{k!}$. Furthermore, we define $V(x, d) := \binom{x}{0} + \binom{x}{1} + \dots + \binom{x}{d}$. In particular if x is a positive integer, $V(x, d)$ is the size of the Hamming ball of radius d in the x-dimensional cube.

▶ **Conjecture 14.** *Let H be an n-vertex d-graph with no clique of size $r + 1$. Then $k(H) \leq V(\frac{(d-1)n}{r}, d - 1)^{\frac{r}{d-1}}$. In particular when $d - 1 \mid r$ and $r \mid (d - 1)n$, the unique extremal case is the $\frac{r}{d-1}$-partite d-graph on n vertices where hyperedges are all d-tuples which intersect each part in at most $d - 1$ vertices.*

Observe that Theorem 13 proves the conjecture for $r \geq (1 - \frac{1}{d})n$. Let us make some comments regarding Conjecture 14 and how it compares with the usual Turán problem for hypergraphs. The Turán problem asks to determine the maximum number of hyperedges in a d-graph with no clique of size $r + 1$. This is notoriously open even for $d = r = 3$. One explanation for the intractability of this problem is that unlike the case of graphs, there are exponentially many extremal examples for hypergraphs (see [19]). In our case however we conjecture that there is a unique extremal example which might mean that the problem is easier. Moreover, for our application we do not need the full generality of the conjecture. In particular, it is sufficient for us to determine the case $d = 3$ and $r = \epsilon n$ for $\epsilon > 0$. Interestingly for some regime of these parameters the Turán number is known and has been rediscovered several times (see [29, 6, 30]).

▶ **Theorem 15.** *Assuming Conjecture 14 holds, $u(n, r, d) \leq V(\frac{(d-1)n}{r}, d - 1)^{\frac{r}{d-1}}$. In particular for every $\epsilon > 0$, $u(n, \epsilon n, 3) \leq (\binom{2/\epsilon}{2} + 2/\epsilon + 1)^{\epsilon n/2}$.*

3 Depth-3 Circuits

In this section we give applications of the $\mathbb{U}_2$ and $\mathbb{U}_3$ dimension to depth-3 circuits.

3.1 Projections

A *projection* in $\{0,1\}^n$ is an affine space given by equations of the form $x = 0$, $x = 1$, $x = y$ or $x = 1 - y$. Given $S \subseteq \{0,1\}^n$, we denote by $\mathbb{PR}(S)$ the dimension of the largest projection contained in S. We define $\mathbb{AF}(S)$ to be the dimension of the largest affine space contained in S. Note that $\mathbb{AF}(S) \geq \mathbb{PR}(S)$ since a projection is a particular type of affine space. We will show that the converse is also true when S is the set of satisfying assignments of a 2-CNF.

A projection of dimension d in a variable set X can be represented as a sequence of $2(d+1)$ sets $(A_0, B_0, A_1, B_1, \ldots, A_d, B_d)$, where $\bigcup\limits_{i=0}^{d} A_i \cup B_i = X$ and for every $i \geq 1$ $A_i \cup B_i$ is non-empty. A_0 contains variables that are set to 0, B_0 contains those set to 1, and for $i \geq 1$ the variables from A_i are equal to each other and the variables from B_i are equal to their negations.

For a Boolean function f, we write $\mathbb{PR}(f)$ to denote $\mathbb{PR}(f^{-1}(1))$.

▶ **Lemma 16** (Paturi, Saks, and Zane [24])**.** *Let $S = \mathrm{sat}(\phi)$ for a 2-CNF formula ϕ. Then $\mathbb{PR}(S) = \mathbb{VC}(S)$.*

Thus, by the Sauer–Shelah lemma, if $\mathbb{PR}(S) \leq d$ for such S, then $|S| \leq \sum_{i=0}^{d} \binom{n}{i}$. We improve this bound by showing that as far as 2-CNFs are concerned, $\mathbb{VC}$ and $\mathbb{U}_2$ dimensions are the same.

▶ **Lemma 17.** *Let $S = \mathrm{sat}(\phi)$ for a 2-CNF formula ϕ. Then $\mathbb{VC}(S) = \mathbb{U}_2(S)$.*

Proof. $\mathbb{VC}(S) \leq \mathbb{U}_2(S)$ follows from the definition. It remains to show that $\mathbb{VC}(S) \geq \mathbb{U}_2(S)$. Let ϕ be the 2-CNF formula in a variable set X with $S = \mathrm{sat}(\phi)$. Recall the *implication digraph* of ϕ, $D(F)$, which is constructed as follows. For every literal u there is a vertex. For every clause $u \vee v$ we have two edges, $\overline{u} \to v$ and $\overline{v} \to u$. Every unit clause v gives the edge $\overline{v} \to v$. We say that literal u *implies* literal v if there is a directed path from u to v. Let $I \subseteq X$ be 2-universal for S. It follows that for any $x, y \in I$ no literal on x implies a literal on y, since otherwise setting a value of one forces the value of the other, contradicting 2-universality. We claim that any assignment to the variables in I can be extended to a full assignment satisfying ϕ. Let α be any satisfying assignment of ϕ. We follow the argument of [24]. There are different types of literals:

- Literals that imply some literal in I: we set such literals to 0.
- Those that are implied by some literal in I: we set these to 1.
- Those that are in the same strongly connected component with some literal in I: we set these as the one in I.
- All other literals: we set these according to α.

It is easy to see that it defines a satisfying assignment. ◀

We need the following lemma.

▶ **Lemma 18.** *Let $S \subseteq \{0,1\}^n$ be a d-dimensional affine space. Then $\mathbb{VC}(S) = d$.*

Proof. Since S is d-dimensional, there exists a full rank matrix $M \in \{0,1\}^{d \times n}$ and $c \in \{0,1\}^n$, such that $S = \{xM + c : x \in \{0,1\}^d\}$. Since M is full rank, there exists a set $L \subseteq [n]$ of d linearly independent columns. Let M_L be the restriction of M to the columns in L. It follows that M_L is a full-rank $d \times d$ matrix. Observe that the projection of S on L is given by $\{xM_L + c : x \in \{0,1\}^d\}$. Since M_L is full-rank, this equals to the whole d-dimensional space. Therefore, L is shattered by S, and we are done. ◀

Combining these lemmas we get the following.

▶ **Theorem 19.** *Let $S = \mathrm{sat}(\phi)$ for a 2-CNF formula ϕ. Then*

$$\mathbb{AF}(S) = \mathbb{VC}(S) = \mathbb{PR}(S) = \mathbb{U}_2(S).$$

The following lemma directly follows from Theorem 7 and Lemma 17.

▶ **Lemma 20.** *Let $S = \mathrm{sat}(\phi)$ for a 2-CNF formula ϕ in n variables. Then*

$$|S| \le \left(\frac{n}{\mathbb{PR}(S)} + 1\right)^{\mathbb{PR}(S)}.$$

Although projections can be used to prove lower bounds on Σ_3^3 circuits, their application is quite limited. As noted in [24], low-density parity-check codes suggested by Gallager [13] can be used to give an example of such a limitation. Let H be a parity-check matrix of such a code. It contains at most 4 ones in each row. Therefore, the system $Hx = 0$ can be represented as a 4-CNF formula. This code has exponentially many codewords and only contains projections of constant size since its distance is linear.

This construction can easily be extended to 3-CNF formulas. Consider any line of the linear system $Hx = 0$ containing exactly four variables. Without loss of generality, we may assume that it depends on variables x_1, x_2, x_3, x_4, i.e., it is $x_1 + x_2 + x_3 + x_4 = 0$. We replace it with two new lines $y + x_3 + x_4 = 0$ and $y = x_1 + x_2$, where y is a fresh extension variable. We do this replacement for every line of $Hx = 0$ with four variables. After this transformation, the new system can be represented as a 3-CNF formula. Since the new extension variables are uniquely determined by the original variables, the new code has the same number of codewords and its distance is at least the distance of the original code. Hence, it can only contain a projection of at most constant size.

However, we show that a 3-CNF with sufficiently many satisfying assignments accepts a projection of linear dimension.

▶ **Lemma 21.** *Let ϕ be a k-CNF formula in a variable set X and let $S = \mathrm{sat}(\phi)$. Assume that $I \subseteq X$ is k-universal for S. Then $X \setminus I$ is a hitting set for ϕ, i.e., every clause $C \in \phi$ intersects $X \setminus I$.*

Proof. Assume that this is not the case and a clause C is entirely contained in I. Assume without loss of generality that $C = x_1 \vee \ldots \vee x_k$. By k-universality of I, S contains an assignment which sets all these variables to 0. However, this assignment falsifies C and hence cannot be in S, which is a contradiction. ◀

▶ **Lemma 22.** *There exists a universal constant $\delta > 0$ such that if ϕ is a 3-CNF in n variables accepting at least $7^{n/3} \simeq 2^{0.936n}$ assignments, then $\mathbb{PR}(\phi) \ge \delta n$. Assuming Conjecture 14 holds, the statement holds (although for a different $\delta > 0$) when ϕ has at least $2^{0.707n}$ satisfying assignments.*

Proof. Let $S = \mathrm{sat}(\phi)$. Since $|S| \ge 7^{n/3}$, Theorem 13 implies that $\mathbb{U}_3(S) \ge 2n/3$. By Lemma 21, ϕ has a hitting set J of size at most $n/3$. Under any restriction σ of J, $\phi|_\sigma$ is a 2-CNF. Choose σ such that $\phi|_\sigma$ has at least $(7/2)^{n/3}$ satisfying assignment. Lemma 20 implies there exists $\delta > 0$ such that $\mathbb{PR}(\phi) \ge \mathbb{PR}(\phi|_\sigma) \ge \delta n$.

Under Conjecture 14, $u(n, 0.296n, 3) \leq 2^{0.706n}$. Thus, if ϕ has at least $2^{0.707n}$ satisfying assignments, then ϕ has a hitting set of size at most $0.704n$. Now we can apply the same argument as above. ◀

3.2 Affine dispersers

Recall that an affine disperser for dimension d is a function, which is not constant under any affine space of dimension d.

▶ **Theorem 23.** *Let $f : \{0,1\}^n \to \{0,1\}$ be an affine disperser for dimension $d+1$. Then*

$$s_3^2(f) \geq \frac{\left|f^{-1}(1)\right|}{\left(\frac{n}{d}+1\right)^d}.$$

Proof. Suppose that $f = \bigvee_{i=1}^{m} \phi_i$, where ϕ_i are 2-CNF formulas. It is clear that $\mathbb{AF}(\phi_i) \leq \mathbb{AF}(f) \leq d$. Let $S_i = \text{sat}(\phi_i)$. Since $\mathbb{AF}(\phi_i) = \mathbb{PR}(\phi_i)$ by Theorem 19, Lemma 20 implies that

$$|S_i| \leq \left(\frac{n}{d}+1\right)^d.$$

Hence,

$$s_3^2(f) \geq m \geq \frac{\left|f^{-1}(1)\right|}{\left(\frac{n}{d}+1\right)^d}.$$ ◀

▶ **Theorem 24.** *Let $f = \{0,1\}^n \to \{0,1\}$ be an affine disperser for dimension $d = o(n)$ with $\left|f^{-1}(1)\right| \geq 2^{n-o(n)}$. Then*

$$s_3^3(f) \geq 2^{0.064n-o(n)}.$$

Furthermore, assuming Conjecture 14 holds,

$$s_3^3(f) \geq 2^{0.293n-o(n)}.$$

Proof. We apply Lemma 22 and follow the same proof as Theorem 23. ◀

3.3 Degree-2 polynomials

We now give a lower bound for all degree-2 polynomials over $\mathbb{F}_2$.

▶ **Lemma 25.** *Let p be a degree-2 polynomial over $\mathbb{F}_2$ in n variables and I a set of variables of p, no two of which produce a monomial of p. Then*

$$s_3^t(p) \geq 2^{\frac{|I|}{2t}}.$$

Proof. We randomly assign the values of the variables not belonging to I and denote the resulting polynomial as q. It is clear that $s_3^t(p) \geq s_3^t(q)$.

By construction of I, q is an affine function in at most $|I|$ variables. If a variable $z \in I$ does not appear in any degree-2 monomial of p, then z always appears in q. Otherwise, z appears in q with probability $\frac{1}{2}$. It follows that the expected number of the variables that appear in q is at least $\frac{|I|}{2}$. Therefore, there exists an assignment, such that q is an affine function in at least $\frac{|I|}{2}$ variables.

The parity function in n variables requires Σ_3^t circuit of size at least $2^{\frac{n}{t}}$ [24]. Thus, $s_3^t(q) \geq 2^{\frac{|I|}{2t}}$. ◀

▶ **Lemma 26.** *Let p be a degree-2 polynomial over $\mathbb{F}_2$ in n variables. Then*

$$s_3^2(f) \geq 2^{n/10}.$$

Proof. Let I be the largest set that satisfies the assumptions of Lemma 25.

If $|I| \geq \beta n$, then

$$s_3^2(p) \geq 2^{\frac{\beta}{4}n}.$$

Otherwise, there are no large projections that make p constant. Consider a projection $(A_0, B_0, A_1, B_1, \dots, A_d, B_d)$ of dimension d, which makes p constant. Let J be the set of all the variables contained in some (A_i, B_i) for $i \geq 1$ with $|A_i \cup B_i| = 1$. J satisfies the conditions for Lemma 25 since otherwise p under the projection would have a monomial with a non-zero coefficient. Thus, $|J| < \beta n$ and every other part (A_i, B_i) contains at least two variables.

Therefore, we have the following:

$$n = \sum_{i=0}^{d} |A_i \cup B_i| \geq |J| + (d - |J|)2 > 2d - \beta n.$$

It gives an upper bound on d:

$$d < \frac{1+\beta}{2} n.$$

This, Theorem 23, and a well-known fact that a degree-2 polynomial over $\mathbb{F}_2$ is 1 on at least 2^{n-2} inputs implies that

$$s_3^2(p) \geq 2^{\left(1-\frac{1+\beta}{2}\log\left(\frac{2}{1+\beta}+1\right)\right)n-o(n)}.$$

By choosing $\beta \approx 0.4$, we conclude that $s_3^2(p) \geq 2^{n/10}$. ◀

4 The inner product and 2-CNF formulas

It is more convenient for us to consider the negation of the inner product function IP on k pairs of variables.

$$\mathrm{IP}(x_1, \dots, x_k, y_1, \dots, y_k) := \begin{cases} 1, & \text{if } \sum\limits_{i=1}^{k} x_i y_i \pmod 2 = 0 \\ 0, & \text{otherwise.} \end{cases}$$

[15] studied the following properties of Boolean circuits. For an integer $k \geq 2$, $\alpha(k)$ is the infimum of all values α such that any circuit of size s can be rewritten as an $\mathrm{OR}_{2^{\alpha s}} \circ \mathrm{AND} \circ \mathrm{OR}_k$ circuit. The exact value is only known for $\alpha(2)$, and they showed that $\alpha(3) \leq \frac{\log_2 3}{4}$. The inner product function is a natural candidate for a hard function for Σ_3^3.

▶ **Lemma 27** ([15]).

1. $2^{\frac{k}{2}} \leq s_3^2(\mathrm{IP}) \leq 2^{k-o(k)}$.
2. $2^{\frac{k}{3}} \leq s_3^3(\mathrm{IP}) \leq 3^{\frac{k}{2}}$.

Both lower bounds are obtained via a simple reduction to the parity function and the fact that $s_3^t(\oplus_n) \geq 2^{\frac{n}{t}}$ [24]. If the upper bound for $s_3^3(\mathrm{IP})$ in the lemma is tight, then $\alpha(3) = \frac{\log_2 3}{4}$. However, the correct bound is not known even for $s_3^2(\mathrm{IP})$.

We say that a CNF formula ϕ is *consistent* with the inner product if $\phi^{-1}(1) \subseteq \mathrm{IP}^{-1}(1)$. We denote this as $\phi \leq \mathrm{IP}$. The 2-universality can be used to prove that every 2-CNF formula consistent with the inner product has at most 3^k satisfying assignments. However, if applied directly, this only gives $2^{0.40k}$ lower bound, which is worse than the reduction to the parity function.

▶ **Theorem 28.** *Let ϕ be a 2-CNF formula consistent with the inner product on k pairs of variables. Then*

$$|\mathrm{sat}(\phi)| \leq 3^k.$$

Proof. Let $S = \mathrm{sat}(\phi)$.

It is well-known that IP is a k-affine disperser (see, e.g., [7]). Thus, $\mathbb{AF}(S) \leq k$. By Theorem 19, $\mathbb{U}_2(S) = \mathbb{AF}(S) \leq k$. Lemma 20 implies that

$$|S| \leq \left(\frac{2k}{k} + 1\right)^k = 3^k. \qquad ◀$$

What is more, the 2-CNF formula that has this many satisfying assignments is unique.

Consider a 2-CNF formula ϕ such that $\phi \leq IP$ and ϕ has the maximal possible number of satisfying assignments. We will prove that there is only one 2-CNF formula that has this many satisfying assignments:

$$\bigwedge_{i=1}^{k} (\neg x_i \vee \neg y_i)\,.$$

A *transitive closure* $\mathrm{tc}(\phi)$ of a CNF formula ϕ is an equivalent CNF formula that contains all clauses that can be derived from ϕ.

▶ **Fact 29.** *Let ϕ be a 2-CNF formula. $\phi \not\models (z = \alpha)$ for every variable z of ϕ and every $a \in \{0,1\}$ if and only if every clause of $\mathrm{tc}(\phi)$ has width 2.*

Without loss of generality we can assume that $\phi = \mathrm{tc}(\phi)$.

We will first prove a general property of 2-CNF formulas consistent with the inner product.

▶ **Lemma 30.** *Consider a 2-CNF formula ϕ that is consistent with inner product on k pairs of variables. Let $J \subseteq [k]\,, J \neq \varnothing$. Suppose that ϕ has two satisfying assignments σ and τ such that:*

- *$\sigma(x_i) = 0$ and $\sigma(y_i) = 1$ for $i \in J$.*
- *$\tau(x_i) = 1$ and $\tau(y_i) = 0$ for $i \in J$.*
- *$\sigma(x_i) = \tau(x_i)$ and $\sigma(y_i) = \tau(y_i)$ for $i \in [k] \setminus J$.*

Then at least one of the following holds:

1. *$\phi \models (x_i y_i = 0)$ for some $i \in J$.*
2. *$\phi \models (x_i = x_j)$ for some distinct $i, j \in J$.*

Proof. Let ρ be the common part of σ and τ (i.e., ρ is a partial assignment to x_i and y_i, where $i \in [k] \setminus J$). Consider the restricted formula $\psi = \phi|_\rho$.

For every variable z of ψ we have $\sigma(z) = \neg\tau(z)$. Therefore, ψ cannot have clauses of length 1.

Fix $i \in J$ and consider the assignment σ' that coincides with σ except for the value of x_i: $\sigma'(x_i) = 1$. This assignment cannot satisfy ψ since we flipped the value of only one monomial $x_i y_i$ without changing anything else. Every clause that is falsified by σ' must contain $\neg x_i$ and have length 2. Thus, it can be either of these:

1. $\neg x_i \vee x_j$ for some $j \in J, j \neq i$.
2. $\neg x_i \vee \neg y_j$ for some $j \in J$.

If there is a clause of the second type with $j = i$, then $\phi \vDash (x_i y_i = 0)$, and it concludes the proof.

If it is not the case, we show that there must be a clause of the first type. Assume the opposite: there is a set $A \subseteq J \setminus \{i\}$ such that $\neg x_i \vee \neg y_j$, where $j \in A$, are the only clauses that are falsified by σ'. Define another assignment σ'' as follows: $\sigma''(y_j) = 0$ if $j \in A$ and $\sigma''(z) = \sigma'(z)$ otherwise. We show that the assignment σ'' satisfies ψ. Firstly, note that by construction it satisfies all the clauses that are falsified by σ'.

Suppose that a clause $y_j \vee \ell$ is not satisfied by σ'', where ℓ is a literal. Observe that for any t, $\ell \neq y_t$ since τ sets every y_t to 0 and τ satisfies ψ. Also, $\ell \neq \neg y_t$, where $t \in A$, since in this case $\sigma''(y_t) = 0$. Hence, $\sigma''(\ell) = \sigma'(\ell)$. We can resolve this clause with $\neg x_i \vee \neg y_j$ and get $\neg x_i \vee \ell$. Thus, $\neg x_i \vee \ell$ must also be unsatisfied by σ'', which is a contradiction to the fact that σ'' satisfies all the clauses falsified by σ'.

On the other hand, $\sum\limits_{i \in J} \sigma'(x_i)\sigma'(y_i) = \sum\limits_{i \in J} \sigma''(x_i)\sigma''(y_i)$. Therefore, σ'' cannot be a satisfying assignment of ψ.

Hence, for every $i \in J$ there exists $j \in J \setminus \{i\}$ such that $\neg x_i \vee x_j$ is a clause of ψ. The conjunction of these clauses implies $x_i = x_j$ for some distinct i and j. ◀

We are now ready to prove the uniqueness of the extremal 2-CNF.

▶ **Theorem 31.** *Let ϕ be a 2-CNF formula consistent with the inner product that has the maximum number of satisfying assignments, i.e., $|\text{sat}(\phi)| = 3^k$. Then for every $i \in [k]$ it holds that $\phi \vDash (x_i y_i = 0)$. Therefore, ϕ is equivalent to $\bigwedge\limits_{i=1}^{k} (\neg x_i \vee \neg y_i)$.*

Proof. We prove the statement by induction on k. The base case $k = 1$ is clear.

For the inductive step, we use Lemma 30.

First we show that it is enough to show that $\phi \vDash (x_i y_i = 0)$ for at least one $i \in [k]$.

▷ Claim 32. Suppose that there exists $i \in [k]$ such that $\phi \vDash (x_i y_i = 0)$. Then for *every* $i \in [k]$ it holds that $\phi \vDash (x_i y_i = 0)$.

Proof. There are three ways of setting $x_i y_i$ to 0. For every satisfying assignment σ of ϕ we have one the following:

- $\sigma(x_i) = \sigma(y_i) = 0$.
- $\sigma(x_i) = 0$ and $\sigma(y_i) = 1$.
- $\sigma(x_i) = 1$ and $\sigma(y_i) = 0$.

Now choose a partial assignment ρ of the variables x_i and y_i, such that the number of satisfying assignments of ϕ that coincide with ρ is maximal. Then $\left|\text{sat}(\phi|_\rho)\right| \geq 3^{k-1}$ and we can apply the inductive hypothesis. ◁

If ϕ has satisfying assignments that satisfy the assumptions of Lemma 30, then either ϕ implies $x_i y_i = 0$ for some $i \in [k]$, and we can apply the claim above, or ϕ implies $x_i = x_j$ for some $i, j \in [k], i \neq j$. In the latter case, we show that ϕ has less than 3^k satisfying assignments. Under this assumption, every satisfying assignment of ϕ satisfies

$$x_i(y_i + y_j) + \sum_{s \in [k] \setminus \{i,j\}} x_s y_s = 0.$$

Let ρ be an arbitrary assignment to x_i, y_i, y_j. By Theorem 31, $\phi|_\rho$ has at most 3^{k-2} satisfying assignments. Therefore, in total ϕ can have no more than $8 \cdot 3^{k-2} < 3^k$ satisfying assignments.

To conclude the proof, we show that if ϕ does not satisfy the assumptions of Lemma 30, then the number of satisfying assignments $|\mathrm{sat}(\phi)|$ is strictly less than 3^k. We want to count the number of satisfying assignments in this case. By the definition of IP, only an even number of monomials $x_i y_i$ can be set to 1. Thus, for every satisfying assignment σ of ϕ there exists a set $I \subseteq [k]$ of even size such that $\sigma(x_i) = \sigma(y_i) = 1$ for $i \in I$ and $\sigma(x_i)\sigma(y_i) = 0$ for $i \notin I$. Let $J \subseteq [k] \setminus I$ be the set of all the indices i satisfying $\sigma(x_i) = \sigma(y_i) = 0$. Since we assume that we cannot apply Lemma 30, there can be at most one satisfying assignment of ϕ for every choice of I and J.

Thus, the total number of satisfying assignments of ϕ with fixed I is as most $2^{k-|I|}$. It follows that

$$|\mathrm{sat}(\phi)| \leq \sum_{\substack{I \subseteq [k] \\ |I| \text{ is even}}} 2^{k-|I|} = \sum_{s=0}^{k/2} \binom{k}{2s} 2^{k-2s} = \frac{1}{2}\left(3^k + 1\right) < 3^k. \qquad \blacktriangleleft$$

5 Conclusion

The most immediate problem which remains open is determining the exact Σ_3^2 and eventually Σ_3^3 complexity of IP. It would be particularly pleasant if this is resolved using a stability argument extending our result on the uniqueness of 2-CNFs consistent with IP with the maximum number of satisfying assignments.

More generally collecting new combinatorial insights on the set of satisfying assignments of k-CNFs seems necessary to make progress towards Σ_3^k lower bounds (and k-SAT which we did not cover in this paper).

Our work immediately raises the following natural question. Can we obtain better Sauer–Shelah lemmas for k-CNFs, i.e., given d, k, n what is the largest size of a set $S \subseteq \{0,1\}^n$ with $\mathbb{VC}(S) = d$ which is the set of satisfying assignments of a k-CNF formula? We showed that for $k = 2$ this bound is $\left(\frac{n}{d} + 1\right)^d$.

References

1 V. E. Alekseev. An upper bound for the number of maximal independent sets in a graph. *Discrete Math. Appl.*, 17(4):355–359, 2007. `doi:doi:10.1515/dma.2007.030`.

2 Noga Alon, Guy Moshkovitz, and Noam Solomon. Traces of hypergraphs. *J. Lond. Math. Soc.*, 100(2):498–517, 2019. `doi:10.1112/jlms.12233`.

3 Eli Ben-Sasson and Swastik Kopparty. Affine dispersers from subspace polynomials. *SIAM J. Comput.*, 41(4):880–914, 2012. `doi:10.1137/110826254`.

4 Béla Bollobás and A. J. Radcliffe. Defect sauer results. *J. Comb. Theory, Ser. A*, 72(2):189–208, 1995.

5 J. Adrian Bondy. Induced subsets. *J. Combinatorial Theory Ser. B*, 12:201–202, 1972. doi:10.1016/0095-8956(72)90025-1.

6 Vasek Chvátal and Colin McDiarmid. Small transversals in hypergraphs. *Comb.*, 12(1):19–26, 1992. doi:10.1007/BF01191201.

7 Gil Cohen and Igor Shinkar. The complexity of DNF of parities. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science, Cambridge, MA, USA, January 14-16, 2016*, pages 47–58. ACM, 2016. doi:10.1145/2840728.2840734.

8 Irit Dinur and Or Meir. Toward the KRW composition conjecture: Cubic formula lower bounds via communication complexity. *Comput. Complex.*, 27(3):375–462, 2018. doi:10.1007/s00037-017-0159-x.

9 Jeff Edmonds, Russell Impagliazzo, Steven Rudich, and Jirí Sgall. Communication complexity towards lower bounds on circuit depth. *Comput. Complex.*, 10(3):210–246, 2001. doi:10.1007/s00037-001-8195-x.

10 Magnus Gausdal Find, Alexander Golovnev, Edward A. Hirsch, and Alexander S. Kulikov. A better-than-3n lower bound for the circuit complexity of an explicit function. In *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, 9-11 October 2016, Hyatt Regency, New Brunswick, New Jersey, USA*, pages 89–98. IEEE Computer Society, 2016. doi:10.1109/FOCS.2016.19.

11 Peter Frankl. On the trace of finite sets. *J. Comb. Theory, Ser. A*, 34(1):41–45, 1983. doi:10.1016/0097-3165(83)90038-9.

12 Zoltán Füredi. A proof of the stability of extremal graphs, simonovits' stability from szemerédi's regularity. *J. Comb. Theory, Ser. B*, 115:66–71, 2015. doi:10.1016/j.jctb.2015.05.001.

13 Robert G. Gallager. Low-density parity-check codes. *IRE Trans. Inf. Theory*, 8(1):21–28, 1962. doi:10.1109/TIT.1962.1057683.

14 Alexander Golovnev, Edward A. Hirsch, Alexander Knop, and Alexander S. Kulikov. On the limits of gate elimination. *J. Comput. Syst. Sci.*, 96:107–119, 2018. doi:10.1016/j.jcss.2018.04.005.

15 Alexander Golovnev, Alexander S. Kulikov, and R. Ryan Williams. Circuit depth reductions. In *12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference*, volume 185 of *LIPIcs*, pages 24:1–24:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.ITCS.2021.24.

16 Russell Impagliazzo, Ramamohan Paturi, and Francis Zane. Which problems have strongly exponential complexity? *J. Comput. Syst. Sci.*, 63(4):512–530, 2001. doi:10.1006/jcss.2001.1774.

17 Stasys Jukna. *Boolean function complexity*, volume 27 of *Algorithms and Combinatorics*. Springer, Heidelberg, 2012. Advances and frontiers. doi:10.1007/978-3-642-24508-4.

18 Peter Keevash. Shadows and intersections: stability and new proofs. *Adv. Math.*, 218(5):1685–1703, 2008. doi:10.1016/j.aim.2008.03.023.

19 A. V. Kostochka. A class of constructions for Turán's (3, 4)-problem. *Combinatorica*, 2(2):187–192, 1982. doi:10.1007/BF02579317.

20 Or Meir. Toward better depth lower bounds: Two results on the multiplexor relation. *Comput. Complex.*, 29(1):4, 2020. doi:10.1007/s00037-020-00194-8.

21 Peter Bro Miltersen, Jaikumar Radhakrishnan, and Ingo Wegener. On converting CNF to DNF. *Theor. Comput. Sci.*, 347(1-2):325–335, 2005. doi:10.1016/j.tcs.2005.07.029.

22 Ramamohan Paturi, Pavel Pudlák, Michael E. Saks, and Francis Zane. An improved exponential-time algorithm for k-SAT. *J. ACM*, 52(3):337–364, 2005. doi:10.1145/1066100.1066101.

23 Ramamohan Paturi, Pavel Pudlák, and Francis Zane. Satisfiability coding lemma. In *38th Annual Symposium on Foundations of Computer Science, FOCS '97, Miami Beach, Florida, USA, October 19-22, 1997*, pages 566–574. IEEE Computer Society, 1997. doi:10.1109/SFCS.1997.646146.

24 Ramamohan Paturi, Michael E. Saks, and Francis Zane. Exponential lower bounds for depth three boolean circuits. *Comput. Complex.*, 9(1):1–15, 2000. doi:10.1007/PL00001598.

25 Benjamin Rossman. Criticality of regular formulas. In *34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA*, volume 137 of *LIPIcs*, pages 1:1–1:28. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. doi:10.4230/LIPIcs.CCC.2019.1.

26 Norbert Sauer. A generalization of a theorem of Turán. *Journal of Combinatorial Theory, Series B*, 10(2):109–112, 1971. doi:10.1016/0095-8956(71)90071-2.

27 Norbert Sauer. On the density of families of sets. *J. Comb. Theory, Ser. A*, 13(1):145–147, 1972. doi:10.1016/0097-3165(72)90019-2.

28 Saharon Shelah. A combinatorial problem; stability and order for models and theories in infinitary languages. *Pacific J. Math.*, 41:247–261, 1972. URL: http://projecteuclid.org/euclid.pjm/1102968432.

29 Alexander Sidorenko. Exact values of Turán numbers. *Mat. Zametki*, 42(5):751–760, 764, 1987.

30 Stéphan Thomassé and Anders Yeo. Total domination of graphs and small transversals of hypergraphs. *Comb.*, 27(4):473–487, 2007. doi:10.1007/s00493-007-2020-3.

31 Leslie G. Valiant. Graph-theoretic arguments in low-level complexity. In *Mathematical foundations of computer science (Proc. Sixth Sympos., Tatranská Lomnica, 1977)*, pages 162–176. Lecture Notes in Comput. Sci., Vol. 53, 1977.

32 Vladimir. N. Vapnik and Alexey. Y. Chervonenkis. On the uniform convergence of relative frequencies of events to their probabilities. *Theory of Probab. and its Applications*, 16(2):264–280, 1971.

33 Alexander Aleksandrovich Zykov. On some properties of linear complexes. *Matematicheskii sbornik*, 66(2):163–188, 1949.