Improved Bounds for the Sunflower Lemma

Ryan Alweiss*
Princeton University
United States
alweiss@math.princeton.edu

Shachar Lovett†
University of California, San Diego
United States
shachar.lovett@gmail.com

Kewen Wu
Peking University
China
shlw_kevin@pku.edu.cn

Jiapeng Zhang‡
Harvard University
United States
jpeng.zhang@gmail.com

ABSTRACT

A sunflower with r petals is a collection of r sets so that the intersection of each pair is equal to the intersection of all. Erdős and Rado proved the sunflower lemma: for any fixed r, any family of sets of size w, with at least about w^w sets, must contain a sunflower. The famous sunflower conjecture is that the bound on the number of sets can be improved to c^w for some constant c. In this paper, we improve the bound to about $(\log w)^w$. In fact, we prove the result for a robust notion of sunflowers, for which the bound we obtain is tight up to lower order terms.

CCS CONCEPTS

• **Mathematics of computing** → **Combinatorics**; • **Theory of computation** → *Pseudorandomness and derandomization*; *Complexity theory and logic.*

KEYWORDS

Robust sunflower lemma, sunflower conjecture, switching lemma

ACM Reference Format:
Ryan Alweiss, Shachar Lovett, Kewen Wu, and Jiapeng Zhang. 2020. Improved Bounds for the Sunflower Lemma. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC '20), June 22–26, 2020, Chicago, IL, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3357713.3384234

1 INTRODUCTION

Let X be a finite set. A set system $\mathcal{F}$ on X is a collection of subsets of X. We call $\mathcal{F}$ a w-set system if each set in $\mathcal{F}$ has size at most w.

Definition 1.1 (Sunflower). A collection of sets $S_1, \ldots, S_r$ is an *r-sunflower* if

$$S_i \cap S_j = S_1 \cap \cdots \cap S_r, \qquad \forall i \neq j.$$

We call $K = S_1 \cap \cdots \cap S_r$ the *kernel* and $S_1 \setminus K, \ldots, S_r \setminus K$ the *petals* of the sunflower.

Erdős and Rado [13] proved that large enough set systems must contain a sunflower. The name "sunflower" is due to Peter Frankl.

Lemma 1.2 (Sunflower lemma [13]). *Let $r \geq 3$ and $\mathcal{F}$ be a w-set system of size $|\mathcal{F}| \geq w! \cdot (r-1)^w$. Then $\mathcal{F}$ contains an r-sunflower.*

Erdős and Rado conjectured in the same paper that the bound in Lemma 1.2 can be drastically improved.

Conjecture 1.3 (Sunflower conjecture [13]). *Let $r \geq 3$. There exists $c(r)$ such that any w-set system $\mathcal{F}$ of size $|\mathcal{F}| \geq c(r)^w$ contains an r-sunflower.*

The bound in Lemma 1.2 is of the form $w^{w(1+o(1)}$ where the $o(1)$ depends on r. Despite nearly 60 years of research, the best known bounds towards the sunflower conjecture were still of the form $w^{w(1+o(1))}$, even for $r = 3$. More precisely, Kostochka [27] proved that any w-set system of size $|\mathcal{F}| \geq cw! \cdot (\log\log\log w / \log\log w)^w$ must contain a 3-sunflower for some absolute constant c. Recently, Fukuyama [17] claimed an improved bound for $r = 3$ to $w^{(3/4+o(1))w}$, but this proof has yet to be verified.

In this paper, we vastly improve the known bounds. We prove that any w-set system of size $(\log w)^{w(1+o(1))}$ must contain a sunflower. More precisely, we obtain the following:

Theorem 1.4 (Main theorem, sunflowers). *Let $r \geq 3$. Any w-set system $\mathcal{F}$ of size $|\mathcal{F}| \geq (\log w)^w (r \cdot \log\log w)^{O(w)}$ contains an r-sunflower.*

1.1 Robust Sunflowers

We consider a "robust" generalization of sunflowers, the study of which was initiated by Rossman [40], who was motivated by questions in complexity theory. Later, it was studied by Lovett, Solomon and Zhang [29] in the context of the sunflower conjecture.

First, we define a more "robust" version of the property of having disjoint sets. Given a finite set X, we denote by $\mathcal{U}(X, p)$ the distribution of sets $Y \subset X$, where each element $x \in X$ is included in Y independently with probability p (there are sometimes referred to as "p-biased distributions").

*Research supported by an NSF Graduate Research Fellowship.
†Research supported by NSF award 1614023.
‡Research Supported by NSF grant CCF-1763299 and Salil Vadhan's Simons Investigator Award.

STOC '20, June 22–26, 2020, Chicago, IL, USA

ACM ISBN 978-1-4503-6979-4/20/06…$15.00
https://doi.org/10.1145/3357713.3384234

Definition 1.5 (Satisfying set system). Let $0 < \alpha, \beta < 1$. A set system $\mathcal{F}$ on X is (α, β)-satisfying if

$$\Pr_{Y \sim \mathcal{U}(X,\alpha)}[\exists S \in \mathcal{F}, S \subset Y] > 1 - \beta.$$

As aforementioned, the property of being satisfying is a robust analogue of the property of having disjoint sets.

Lemma 1.6 ([29]). *If $\mathcal{F}$ is a $(1/r, 1/r)$-satisfying set system and $\emptyset \notin \mathcal{F}$, then $\mathcal{F}$ contains r pairwise disjoint sets.*

Proof. Let $\mathcal{F}$ be a set system on X. Consider a random r-coloring of X, where each element obtains any of the r colors with equal probability. Let $Y_1, \dots, Y_r$ denote the color classes, which are a random partition of X. For $i = 1, \dots, r$, let $\mathcal{E}_i$ denote the event that $\mathcal{F}$ contains an i-monochromatic set, namely,

$$\mathcal{E}_i = [\exists S \in \mathcal{F}, S \subset Y_i].$$

Note that $Y_i \sim \mathcal{U}(X, 1/r)$, and since we assume $\mathcal{F}$ is $(1/r, 1/r)$-satisfying, we have

$$\Pr[\mathcal{E}_i] > 1 - 1/r.$$

By the union bound, with positive probability all $\mathcal{E}_1, \dots, \mathcal{E}_r$ hold. In this case, $\mathcal{F}$ contains a set which is i-monochromatic for each $i = 1, \dots, r$. Such sets must be pairwise disjoint. □

Given a set system $\mathcal{F}$ on X and a set $T \subset X$, the *link* of $\mathcal{F}$ at T is

$$\mathcal{F}_T = \{S \setminus T : S \in \mathcal{F}, T \subset S\}.$$

We now formally define a *robust sunflower* (which was called a *quasi-sunflower* in [40] and an *approximate sunflower* in [29]).

Definition 1.7 (Robust sunflower). Let $0 < \alpha, \beta < 1$, $\mathcal{F}$ be a set system, and let $K = \bigcap_{S \in \mathcal{F}} S$ be the common intersection of all sets in $\mathcal{F}$. $\mathcal{F}$ is an (α, β)-robust sunflower if (i) $K \notin \mathcal{F}$; and (ii) $\mathcal{F}_K$ is (α, β)-satisfying. We call K the *kernel*.

Lemma 1.8 ([29]). *Any $(1/r, 1/r)$-robust sunflower contains an r-sunflower.*

Proof. Let $\mathcal{F}$ be a $(1/r, 1/r)$-robust sunflower, and let $K = \bigcap_{S \in \mathcal{F}} S$ be the common intersection of the sets in $\mathcal{F}$. Note that by assumption, $\mathcal{F}_K$ does not contain the empty set as an element. Lemma 1.6 gives that $\mathcal{F}_K$ contains r pairwise disjoint sets $S_1, \dots, S_r$. Thus $S_1 \cup K, \dots, S_r \cup K$ is an r-sunflower in $\mathcal{F}$. □

The proof of Theorem 1.4 follows from the following stronger theorem, by setting $\alpha = \beta = 1/r$ and applying Lemma 1.8. The theorem verifies a conjecture raised in [29], and answers a question of [40].

Theorem 1.9 (Main theorem, robust sunflowers). *Let $0 < \alpha, \beta < 1$. Any w-set system $\mathcal{F}$ of size $|\mathcal{F}| \geq (\log w)^w \cdot (\log\log w \cdot \log(1/\beta)/\alpha)^{O(w)}$ contains an (α, β)-robust sunflower.*

The bound of $(\log w)^{w(1+o(1))}$ for robust sunflowers is sharp; it cannot be improved beyond $(\log w)^{w(1-o(1))}$. We give an example demonstrating this in Lemma 2.1.

1.2 Connections to Computer Science

The sunflower lemma has had many applications in mathematics and computer science. Here we briefly discuss some of the computer science applications. While it is reasonable to assume that some of the bounds obtained using the sunflower lemma can be improved using our new results, we have not attempted a thorough literature survey to see which ones can be improved, and leave this for future work.

Circuit lower bounds. Alon, Karchmer, and Wigderson [1] used the sunflower lemma to prove a lower bound for the number of wires in a circuit that computes the Hadamard transform by depth-2 circuits. Jukna [25] extended this work, and also used the sunflower lemma to prove similar lower bounds for approximating the Hadamard transform. As aforementioned, Rossman [40] defined robust sunflowers, motivated by an application to monotone circuit lower bounds. The improved (robust) sunflower lemma has been used by Cavalar, Kumar, and Rossman [6] to improve previous monotone circuit lower bounds.

Hardness of approximation. Dinur and Safra [11] used sunflowers in the soundness analysis of their proof of hardness of approximation for the Minimum Vertex Cover problem.

Matrix multiplication. Alon et al. [2] studied variants of the sunflower conjecture and their connections with fast matrix multiplication algorithms.

Pseudorandomness. Gopalan, Meka, and Reingold [20] used the robust sunflowers for DNF sparsification, which gives better pseudorandom generators fooling small-width DNFs and faster deterministic algorithm counting satisfying assignments of DNFs.

Cryptography. Luby et al.[32] studied broadcast encryption system, and proved a trade-off between the number of establishment keys held by each user and the number of transmissions needed to establish a new broadcast key, where their lower bounds relies on the sunflower lemma. Naor et al.[35] extended this to a wider regime of parameters. Gentry et al.[19] proved that the bounds are optimal using a weaker notion of sunflowers.

Dachman-Soled et al. [8] studied locally decodable and updatable non-malleable codes. They showed that a sunflower structure in the codewords allows for a rewind attack.

Komargodski et al. [26] showed that finding a sunflower (or a pair of duplicate sets), where the underlying set system is given by the output of a succinct circuit, is hard assuming the existence of collision resistant hash functions.

Data structure lower bound. In the bit probe model, Frandsen et al. [15] used the sunflower lemma to prove lower bounds for dynamic word problems, Mortensen et al. [34] used it to prove trade-offs in two stage greater-than functions, and Rahman [37] used it to analyze the increment operation for integers.

In cell probe model, Gal et al. [18] used the sunflower lemma to prove lower bounds for the redundancy/query time trade-off of solutions to static data structure problems, and Natarajan et al. [36] used a weaker notion of sunflowers to analyze non-adaptive data structures computing the minimum, median, and predecessor.

In the CRCW PRAM model, the sunflower lemma was used to prove lower bounds by Berkman et al. [5] and incomparability results by Grolmusz et al. [21] in various models.

Property testing. Haviv et al. [23] showed that a refutation of a variant of the sunflower conjecture implies a super-polynomial lower bound on the query complexity of the canonical tester for cycle freeness. Balaji et al. [4] used the sunflower lemma to obtain lower bounds on the query complexity of graph properties in the node query setting.

Fixed parameter complexity. The sunflower lemma is a common kernelization technique used in FPT algorithms [7, 12]. For example, it was used for hitting set problems by Flum et al. [14], for constraint satisfaction problem under finite Boolean constraint families by Marx et al. [33], for the subgraph test problem by Jansen et al. [24], and for set matching problems by Dell et al. [9]. The last two works also use it for graph packing problems.

Thresholds in random graphs. The technique developed in this paper has been used by Frankston, Kahn, Narayanan, and Park [16] to resolve a conjecture of Talagrand in random graph theory.

1.3 Proof Overview

In this section, we explain the high level ideas underlying the proof of Theorem 1.9. Our framework builds upon the work of Lovett, Solomon and Zhang [29]. Their main idea was to apply a structure vs. pseudo-randomness approach. However, the proof relied on a certain conjecture on the level of pseudo-randomness needed for the argument to go through. Our main technical result is a resolution of this conjecture.

To be concrete, we consider the problem of finding a 3-sunflower, which corresponds in our framework to finding a $(1/3, 1/3)$-robust sunflower (see Lemma 1.8). Given $w \geq 2$, our goal is to find a parameter $\kappa = \kappa(w)$ such that any w-set system of size κ^w must contain a $(1/3, 1/3)$-robust sunflower, and hence also a 3-sunflower.

Recall the definition of links: $\mathcal{F}_T = \{S \setminus T : S \in \mathcal{F}, T \subset S\}$. We say that a w-set system is κ-bounded if (i) $|\mathcal{F}| \geq \kappa^w$; and (ii) $|\mathcal{F}_T| \leq \kappa^{w-|T|}$ for all non-empty T (The actual definition needed in the proof is more delicate, see Definition 3.1 for details).

Let $\mathcal{F}$ be a w-set system of size $|\mathcal{F}| \geq \kappa^w$. Then either $\mathcal{F}$ is κ-bounded, or otherwise there is a link $\mathcal{F}_T$ of size $|\mathcal{F}_T| \geq \kappa^{w-|T|}$. In the latter "structured" case, we can pass to the link and apply induction. (This argument is implicit in the proof of Lemma 3.4.)

Thus it suffices to consider the "pseudo-random" case of w-set systems which are κ-bounded. In [28, 29], it was conjectured that for some absolute C, a $(\log w)^C$-bounded $\mathcal{F}$ is necessarily $(1/3, 1/3)$-satisfying. We show that there is some $\kappa = (\log w)^{1+o(1)}$ is sufficient (see Theorem 3.5), which represents our main technical contribution. This completes the proof of Theorem 1.9. We also show that $\kappa = (\log w)^{1-o(1)}$ is necessary (see Lemma 2.1), so this is tight.

We next explain how we obtain the bound on κ. Let $\mathcal{F}$ be a w-set system which is κ-bounded. In [29] it was conjectured that there exists a $(w/2)$-set system $\mathcal{F}'$ that "covers" $\mathcal{F}$; for any set $S \in \mathcal{F}$, there exists $S' \in \mathcal{F}'$ such that $S' \subset S$, and $\mathcal{F}'$ is κ'-bounded for $\kappa' \approx \kappa$. If this conjecture is true, then it is sufficient to prove that $\mathcal{F}'$ is $(1/3, 1/3)$-satisfying, as this would imply that $\mathcal{F}$ is also $(1/3, 1/3)$-satisfying (in the language of [29], this corresponds to "upper bound compression for DNFs". For more details on the connection to DNF compression see [29–31]).

What we show is that this conjecture is true with two modifications: we are allowed to remove a small fraction of the sets in $\mathcal{F}$, and also remove a small random fraction of the elements in the base set X. To be more precise, sample $W \sim \mathcal{U}(X, p)$ for $p = O(1/\log w)$. We show that with high probability over W, for most sets $S \in \mathcal{F}$, there exists a set $S' \in \mathcal{F}$ such that: (i) $S' \setminus W \subset S \setminus W$; and (ii) $|S' \setminus W| \leq w/2$. Thus we can move to study the set system $\mathcal{F}'$ comprised of the $S' \setminus W$ above, which "approximately covers" $\mathcal{F}$. Note that $\mathcal{F}'$ is a $(w/2)$-set system which is κ'-bounded for $\kappa' \approx \kappa$. In the actual proof, we will replace $w/2$ with $(1-\varepsilon)w$ for a small ε to improve the bounds. For details see Lemma 3.6. Applying this "reduction step" iteratively $t = \log w$ times reduces the size w drastically, and then we can apply standard tools (Janson's inequality, see Lemma 3.9). We get that if we sample $W_1, \ldots, W_t \sim \mathcal{U}(X, p)$ (formally, they are disjoint, but we ignore this detail here), then with good probability there exists $S \in \mathcal{F}$ such that $S \subset W_1 \cup \cdots \cup W_t$. Setting $p \cdot t = 1/3$ and the good probability to be $2/3$ gives that $\mathcal{F}$ is $(1/3, 1/3)$-satisfying, as desired.

To conclude, let us comment on how we prove the reduction step (Lemma 3.6). The main idea is to use an encoding lemma, inspired by Razborov's proof of Håstad's switching lemma [22, 39]. Concretely, for $W \subset X$ and $S \in \mathcal{F}$, we say that the pair (W, S) is *bad* if there is no $S' \in \mathcal{F}$ such that (i) $S' \setminus W \subset S \setminus W$; and (ii) $|S' \setminus W| \leq w/2$. We show that bad pairs can be efficiently encoded, crucially relying on the κ-boundedness condition. This allows to show that for a random W it is very unlikely that there will be many bad sets. The $(w/2)$-set system $\mathcal{F}'$ is then taken to be $\mathcal{F}' = \{S' \setminus W : S' \in \mathcal{F}, |S' \setminus W| \leq w/2\}$.

1.4 Other Related Works

Other than the works already mentioned, there are two more related works that should be mentioned. The term "sunflower" was coined by Deza and Frankl [10], as the original term used by Erdős and Rado was Δ-systems. After the current work was made available on the arXiv, Rao [38] simplified the proof using information theory techniques.

Paper organization. We give an example showing that our bounds for robust sunflowers are essentially tight in Section 2. We prove our main technical result, Theorem 1.9, in Section 3.

2 LOWER BOUND FOR ROBUST SUNFLOWERS

In this section, we construct an example of a w-set system without robust sunflower, even though it has size $(\log w)^{w(1-o(1))}$. For concreteness we fix $\alpha = \beta = 1/2$, but the construction can be easily modified for any other constant values of α, β. We assume that w is large enough.

Lemma 2.1. *There exists a w-set system of size $((\log w)/8)^{w-\sqrt{w}} = (\log w)^{w(1-o(1))}$ which does not contain a $(1/2, 1/2)$-robust sunflower.*

Let $c \geq 1$ be determined later. Let $X_1, \ldots, X_w$ be pairwise disjoint sets of size $m = \log(w/c)$, and let X be their union. Let $\widehat{\mathcal{F}} = X_1 \times \cdots \times X_w$ be the w-set system containing all sets which contain exactly one element from each of the X_i. We first argue that $\widehat{\mathcal{F}}$ is not satisfying.

Claim 2.2. *For $c \geq 1$, $\widehat{\mathcal{F}}$ is not $(1/2, 1/2)$-satisfying.*

Proof. Let $Y \sim \mathcal{U}(X, 1/2)$. We analyze the probability that some X_i is disjoint from Y, which implies that no set in $\widehat{\mathcal{F}}$ is contained in Y. The probability is $1 - (1 - 2^{-m})^w = 1 - (1 - c/w)^w$, which is more than $1/2$ for $c \geq 1$. □

Unfortunately, $\widehat{\mathcal{F}}$ does contain a $(1/2, 1/2)$-robust sunflower with a large kernel. For example, if T contains exactly one element from each of $X_1, \ldots, X_{w-1}$, then $\widehat{\mathcal{F}}_T$ is isomorphic to X_w, and in particular is $(1/2, 1/2)$-satisfying.

To overcome this, let $\varepsilon > 0$ be determined later, and choose $\mathcal{F} \subset \widehat{\mathcal{F}}$ to be a subsystem that satisfies:

$$|S \cap S'| \leq (1 - \varepsilon)w, \qquad \forall S, S' \in \mathcal{F}, S \neq S'.$$

For example, we can obtain $\mathcal{F}$ by a greedy procedure, each time choosing an element S in $\widehat{\mathcal{F}}$ and deleting all S' such that $|S \cap S'| > (1 - \varepsilon)w$. The number of such S' is at most $\binom{w}{\varepsilon w} m^{\varepsilon w} \leq 2^w m^{\varepsilon w}$. Hence we can obtain $\mathcal{F}$ of size $|\mathcal{F}| \geq 2^{-w} m^{(1-\varepsilon)w}$.

Claim 2.3. *For $c \geq 1/\varepsilon$, $\mathcal{F}$ does not contain a $(1/2, 1/2)$-robust sunflower.*

Proof. Consider any set $K \subset X$. We need to prove that $\mathcal{F}$ does not contain a $(1/2, 1/2)$-robust sunflower with kernel K. If it does, $\mathcal{F}_K$ must contain at least two sets, which implies that $|K \cap X_i| \leq 1$ for all i, and that in addition $|K| \leq (1 - \varepsilon)w$. However, in this case we claim even $\widehat{\mathcal{F}}_K$ is not $(1/2, 1/2)$-satisfying.

To prove this, let $I = \{i : |K \cap X_i| = 0\}$ where $|I| \geq \varepsilon w$. Let $Y \sim \mathcal{U}(X, 1/2)$. The probability that there exists $i \in I$ such that Y is disjoint from X_i is $1 - (1 - 2^{-m})^{|I|} \geq 1 - (1 - c/w)^{\varepsilon w}$ which is more than $1/2$ for $c \geq 1/\varepsilon$. □

To conclude the proof of Lemma 2.1 we optimize the parameters. Set $c = 1/\varepsilon$. We have $|\mathcal{F}| \geq 2^{-w}(\log(\varepsilon w))^{(1-\varepsilon)w}$. Setting $\varepsilon = 1/\sqrt{w}$ gives $|\mathcal{F}| \geq ((\log w)/8)^{w-\sqrt{w}} = (\log w)^{(1-o(1))w}$.

3 PROOF OF THEOREM 1.9

We proceed to prove Theorem 1.9. The main idea is to apply a structure vs. pseudo-randomness paradigm, following the approach outlined in [29]. Let $\mathcal{F}$ be a set system, and let $\sigma : \mathcal{F} \mapsto \mathbb{Q}_{\geq 0}$ be a weight function that assigns non-negative rational weights to sets in $\mathcal{F}$ which are not all 0. For simplicity, we do not permit irrational weights. We call the pair $(\mathcal{F}, \sigma)$ a *weighted set system*. For a subset $\mathcal{F}' \subset \mathcal{F}$ we write $\sigma(\mathcal{F}') = \sum_{S \in \mathcal{F}'} \sigma(S)$ the sum of the weights of the sets in $\mathcal{F}'$.

A *weight profile* is a vector $\mathbf{s} = (s_0; s_1, \ldots, s_k)$ where $1 \geq s_0 \geq s_1 \geq \cdots \geq s_k \geq 0$ are rational numbers. We assume implicitly that $s_i = 0$ for all $i > k$.

Definition 3.1 (Bounded weighted set system). Let $\mathbf{s}$ be a weight profile that $\mathbf{s} = (s_0; s_1, \ldots, s_w)$. A weighted set system $(\mathcal{F}, \sigma)$ is $\mathbf{s}$-bounded if

(i) $\sigma(\mathcal{F}) \geq s_0$;
(ii) $\sigma(\mathcal{F}_T) \leq s_{|T|}$ for any link $\mathcal{F}_T$ with non-empty T.

In particular, $\mathcal{F}$ is a w-set system.

Definition 3.2 (Bounded set system). Let $\mathbf{s}$ be a weight profile. A set system $\mathcal{F}$ is $\mathbf{s}$-bounded if there exists a weight function $\sigma : \mathcal{F} \mapsto \mathbb{Q}_+$ such that $(\mathcal{F}, \sigma)$ is $\mathbf{s}$-bounded.

We note that one may always normalize a weight profile to have $s_0 = 1$. However, keeping s_0 as a free parameter helps to simplify some of the arguments later.

The main idea is to show that set systems which are $\mathbf{s}$-bounded, for $\mathbf{s}$ appropriately chosen, are "random looking" and in particular must be (α, β)-satisfying. This motivates the following definition.

Definition 3.3 (Satisfying weight profile). Let $0 < \alpha, \beta < 1$. A weight profile $\mathbf{s}$ is (α, β)-satisfying if any $\mathbf{s}$-bounded set system is (α, β)-satisfying.

The following lemma underlies our proof of Theorem 1.9. This is implicitly where the "induction" on the "structured part" of the set family is occurring.

Lemma 3.4. *Let $0 < \alpha, \beta < 1$ and $w \geq 2$. Let $\kappa = \kappa(w) > 1$ be a non-decreasing function of w such that the weight profile $(1; \kappa^{-1}, \ldots, \kappa^{-\ell})$ is (α, β)-satisfying for all $\ell = 1, \ldots, w$. Then any w-set system $\mathcal{F}$ of size $|\mathcal{F}| > \kappa^w$ must contain an (α, β)-robust sunflower.*

Proof. Assume a contradiction, and let $\mathcal{F}$ be a w-set system on X of size $|\mathcal{F}| > \kappa^w$ without an (α, β)-robust sunflower. Choose $\mathcal{F}$ to minimize w. Let $K \subset X$ be maximal so that $|\mathcal{F}_K| > \kappa^{w-|K|}$. Note that we cannot have $|K| = w$, as in this case $|\mathcal{F}_K| = 1 = \kappa^0$, and so $|K| \leq w-1$. Let $\mathcal{F}' = \mathcal{F}_K \setminus \{\emptyset\}$. Note that $|\mathcal{F}'| \geq \kappa^{w-|K|}$, where for any non-empty set T disjoint from K, $|\mathcal{F}'_T| = |\mathcal{F}_{K \cup T}| \leq \kappa^{w-|K|-|T|}$. Let $\sigma(S) = 1/|\mathcal{F}'|$ for $S \in \mathcal{F}'$. Then $(\mathcal{F}', \sigma)$ is $(1; \kappa^{-1}, \ldots, \kappa^{-\ell})$-bounded for $\ell = w - |K|$, so by minimality, $\mathcal{F}'$ is (α, β)-satisfying, and hence $\{S \cup K : S \in \mathcal{F}'\}$ is an (α, β)-robust sunflower contained in $\mathcal{F}$. □

Lemma 3.4 motivates the following definition. For $0 < \alpha, \beta < 1$ and $w \geq 2$, let $\kappa(w, \alpha, \beta)$ be the least κ such that $(1; \kappa^{-1}, \ldots, \kappa^{-w})$ is (α, β)-satisfying. Theorem 1.9 follows by combining Lemma 3.4 with the following theorem, which bounds $\kappa(w, \alpha, \beta)$.

Theorem 3.5. $\kappa(w, \alpha, \beta) \leq \log w \cdot (\log \log w \cdot \log(1/\beta)/\alpha)^{O(1)}$.

We note that Theorem 3.5 proves a conjecture raised in [29]. We prove Theorem 3.5 in the remainder of this section.

3.1 A Reduction Step

Let $\mathcal{F}$ be a w-set system on X, and fix $w' \leq w$. The main goal in this section is to reduce $\mathcal{F}$ to a w'-set system $\mathcal{F}'$. We prove the following lemma in this section.

Lemma 3.6. *Let $\mathbf{s} = (s_0; s_1, \ldots, s_w)$ be a weight profile, $w' \leq w$, $\delta > 0$ and define $\mathbf{s}' = ((1 - \delta)s_0; s_1, \ldots, s_{w'})$. Assume $\mathbf{s}'$ is (α', β')-satisfying. Then for any $p > 0$, $\mathbf{s}$ is (α, β)-satisfying for*

$$\alpha = p + (1 - p)\alpha', \quad \beta = \beta' + \frac{(4/p)^w s_{w'}}{\delta s_0}.$$

Let $W \subset X$. Given a set $S \in \mathcal{F}$, the pair (W, S) is said to be *good* if there exists a set $S' \in \mathcal{F}$ (possibly with $S' = S$) such that

(i) $S' \setminus W \subset S \setminus W$.
(ii) $|S' \setminus W| \leq w'$.

If no such S' exists, we say that (W, S) is *bad*. Note that if W contains a set in $\mathcal{F}$ (i.e. $S' \subset W$ for some $S' \in \mathcal{F}$) then all pairs (W, S) are good.

Lemma 3.7. *Let $(\mathcal{F}, \sigma)$ be an $\mathbf{s} = (s_0; s_1, \ldots, s_w)$-bounded weighted set system on X. Let $W \subset X$ be a uniform subset of size $|W| = p|X|$ and $\mathcal{B}(W) = \{S \in \mathcal{F} : (W, S) \text{ is bad}\}$. Then $\mathbb{E}_W[\sigma(\mathcal{B}(W))] \leq (4/p)^w s_{w'}$.*

Proof. First, we simplify the setting a bit. We may assume by scaling σ and $\mathbf{s}$ by the same factor that $\sigma(S) = N_S, S \in \mathcal{F}$ are all integers. Let $N = \sum N_S \geq s_0$. We can identify $(\mathcal{F}, \sigma)$ with the multi-set system $\mathcal{F}' = \{S_1, \ldots, S_N\}$, where every set $S \in \mathcal{F}$ is repeated N_S times. Observe that $|\mathcal{F}'_T| = \sigma(\mathcal{F}_T)$ and that (W, S) is bad in $\mathcal{F}$ iff (W, S_i) is bad in $\mathcal{F}'$ where $S_i = S$ is any copy of S. Thus

$$\sigma(\mathcal{B}(W)) = |\{i : S_i \in \mathcal{F}' \text{ and } (W, S_i) \text{ is bad}\}|.$$

Assume that (W, S_i) is bad in $\mathcal{F}'$. In particular, this means that W does not contain any set in $\mathcal{F}$. We describe (W, S_i) with a small amount of information. Let $|X| = n$ and $|W| = pn$. We encode (W, S_i) as follows:

(1) The first piece of information is $W \cup S_i$. The number of options for this is
$$\sum_{i=0}^{w} \binom{n}{pn + i} \leq \binom{n + w}{pn + w} \leq p^{-w} \binom{n}{pn}.$$
(2) Given $W \cup S_i$, let j be minimal such that $S_j \subset W \cup S_i$; in particular, this is equivalent to $S_j \setminus W \subset S_i \setminus W$. There are fewer than 2^w possibilities for $A = S_i \cap S_j$ given that we know S_j. As such, we will let A be the second piece of information.
(3) Note that as (W, S_i) is bad, $|A| = |S_j \setminus W| > w'$. So we know a subset A of S_i of size larger than w'. The number of the sets in $\mathcal{F}'$ which contain A is $|\mathcal{F}'_A| \leq s_{w'}$. The third piece of information will be which one of these is S_i.
(4) Finally, once we have specified S_i, we will specify $S_i \cap W$, which is of course one of 2^w possible subsets of S_i.

From these four pieces of information one can uniquely reconstruct (W, S_i). Thus the total number of bad pairs (W, S_i) is bounded by
$$p^{-w} \binom{n}{pn} \cdot 2^w \cdot s_{w'} \cdot 2^w = (4/p)^w s_{w'} \binom{n}{pn}.$$
The number of sets $W \subset X$ of size $|W| = p|X|$ is $\binom{n}{pn}$. The lemma follows by taking expectation over W. □

The following is a corollary of Lemma 3.7, where we replace sampling $W \subset X$ of size $|W| = p|X|$ with sampling $W \sim \mathcal{U}(X, p)$.

Corollary 3.8. *Let $(\mathcal{F}, \sigma)$ be an $\mathbf{s} = (s_0; s_1, \ldots, s_w)$-bounded weighted set system on X. Let $W \sim \mathcal{U}(X, p)$ and $\mathcal{B}(W) = \{S \in \mathcal{F} : (W, S) \text{ is bad}\}$. Then $\mathbb{E}_W[\sigma(\mathcal{B}(W))] \leq (4/p)^w s_{w'}$.*

Proof. The proof is by a reduction to Lemma 3.7. Replace the base set X with a much larger set X' (without changing $\mathcal{F}$, so the new elements do not belong to any set in $\mathcal{F}$). Let $W' \subset X'$ be a uniform set of size $|W'| = p|X'|$, and let $W = W' \cap X$. Then as X' gets bigger, the distribution of W' approaches $\mathcal{U}(X, p)$, while the conclusion of the lemma depends only on W. □

Proof of Lemma 3.6. Let $(\mathcal{F}, \sigma)$ be an $\mathbf{s}$-bounded weighted set system on X and $\mathbf{s} = (s_0; s_1, \ldots, s_w)$. Let $W \sim \mathcal{U}(X, p)$. Say that W is δ-bad if $\sigma(\mathcal{B}(W)) \geq \delta s_0$. By applying Corollary 3.8 and Markov's inequality, we obtain that

$$\Pr[W \text{ is } \delta\text{-bad}] \leq \frac{\mathbb{E}[\sigma(\mathcal{B}(W))]}{\delta s_0} \leq \frac{(4/p)^w s_{w'}}{\delta s_0}.$$

Fix W which is not δ-bad. By assumption, if (W, S) is good for $S \in \mathcal{F}$, then there exists $\pi(S) = S' \in \mathcal{F}$ (possibly with $S' = S$) such that (i) $S' \setminus W \subset S \setminus W$ and (ii) $|S' \setminus W| \leq w'$. Choose such π with the smallest possible image so that if S', S'' in the image of π are distinct then $S' \setminus W \neq S'' \setminus W$.

Define a new weighted set system $(\mathcal{F}', \sigma')$ on $X' = X \setminus W$ as follows:

$$\mathcal{F}' = \{\pi(S) \setminus W : S \in \mathcal{F} \setminus \mathcal{B}(W)\}, \quad \sigma'(S' \setminus W) = \sigma(\pi^{-1}(S')).$$

We claim that $\mathcal{F}'$ is $\mathbf{s}' = ((1 - \delta)s_0; s_1, \ldots, s_{w'})$-bounded. To see that, note that $\sigma'(\mathcal{F}') = \sigma(\mathcal{F} \setminus \mathcal{B}(W)) \geq (1 - \delta)s_0$ and that for any set $T \subset X'$,

$$\sigma'(\mathcal{F}'_T) = \sum_{S' \supset T} \sigma'(S') = \sum_{S : \pi(S) \supset T} \sigma(S) \leq \sum_{S \supset T} \sigma(S) = \sigma(\mathcal{F}_T) \leq s_{|T|}.$$

Finally, all sets in $\mathcal{F}'$ have size at most w'. Thus, if we choose $W' \sim \mathcal{U}(X', \alpha')$ then we obtain that with probability more than $1 - \beta'$, there exist $S^* \in \mathcal{F}'$ such that $S^* \subset W'$. Recall that $S^* = S \setminus W$ for some $S \in \mathcal{F}$. Thus $S \subset W \cup W'$, which is distributed according to $\mathcal{U}(X, p + (1 - p)\alpha')$. □

3.2 A Final Step

In this section, we directly show that bounded set systems (with very good bounds) are satisfying. A similar argument appears in [40].

Lemma 3.9. *Let $0 < \alpha, \beta < 1$, $w \geq 2$, and set $\kappa = (2 + 4\ln(1/\beta)) \cdot w/\alpha$. Let $(\mathcal{F}, \sigma)$ be an $\mathbf{s} = (s_0; s_1, \ldots, s_w)$-bounded weighted set system where $s_i < \kappa^{-i} \cdot s_0$. Then $\mathcal{F}$ is (α, β)-satisfying.*

Proof. We can assume by scaling that $N_S = \sigma(S)$ for $S \in \mathcal{F}$ are all integers. Let $\widehat{\mathcal{F}}$ be the multi-set system, where each $S \in \mathcal{F}$ is repeated N_S times and $|\mathcal{F}| > \kappa^w$. Then we may also assume that all sets in $\widehat{\mathcal{F}}$ have size exactly w, by adding different dummy elements to each set of size below w. Let $N = \sum N_S \geq s_0$ and denote $\mathcal{F}' = \{S_1, \ldots, S_N\}$, where each S_i is of width w. Note that this $\mathcal{F}'$ satisfies the assumption of the lemma, and that for any set $W \subset X$, if W contains a set of $\mathcal{F}'$ then it also contains a set of $\mathcal{F}$.

The proof is by Janson's inequality (see for example [3, Theorem 8.1.2]). Let $W \sim \mathcal{U}(X, \alpha)$ and $\mathcal{Z}_i$ be the indicator variable for $S_i \subset W$. Denote $i \sim j$ if S_i, S_j intersect. Define

$$\mu = \sum_i \mathbb{E}[\mathcal{Z}_i], \qquad \Delta = \sum_{i \sim j} \mathbb{E}[\mathcal{Z}_i \mathcal{Z}_j].$$

We have $\mu = N\alpha^w$. To compute Δ, let p_ℓ denote the fraction of pairs (i, j) such that $|S_i \cap S_j| = \ell$. Then

$$\Delta = \sum_{\ell=1}^{w} p_\ell N^2 \alpha^{2w-\ell}.$$

To bound p_ℓ, note that for each $S_i \in \mathcal{F}$, and any $R \subset S_i$ of size $|R| = \ell$, the number of $S_j \in \mathcal{F}$ such that $R \subset S_j$ is $|\mathcal{F}_R| \le N/\kappa^{|R|}$. Thus we can bound

$$\Delta \le \sum_{\ell=1}^{w} \binom{w}{\ell} \kappa^{-\ell} N^2 \alpha^{2w-\ell} \le \sum_{\ell=1}^{w} \left(\frac{w}{\alpha\kappa}\right)^{\ell} \mu^2.$$

Let $\kappa = qw/\alpha$ for $q \ge 2$. Then $\Delta \le 2\mu^2/q$. Note that in addition $\Delta \ge \mu$, as we include in particular the pairs (i,i) in Δ. Thus by Janson's inequality,

$$\Pr[\forall i, \mathcal{Z}_i = 0] \le \exp\left\{-\frac{\mu^2}{2\Delta}\right\} \le \exp\left\{-\frac{q}{4}\right\}.$$

The lemma follows by setting $q = 2 + 4\ln(1/\beta)$. □

3.3 Putting Everything Together

We prove Theorem 3.5 in this subsection, where our goal is to bound $\kappa(w, \alpha, \beta)$. We will apply Lemma 3.6 iteratively, until we decrease w enough to apply Lemma 3.9.

Fix $w \ge 2$ throughout, and let $\kappa > 1$ to be optimized later. We first introduce some notation. For $0 < \Delta < 1, \ell \ge 1$, define weight profile $\mathbf{s}(\Delta, \ell) = (1-\Delta; \kappa^{-1}, \dots, \kappa^{-\ell})$. Let $A(\Delta, \ell), B(\Delta, \ell)$ be bounds such that any $\mathbf{s}(\Delta, \ell)$-bounded set system is $(A(\Delta, \ell), B(\Delta, \ell))$-satisfying.

Lemma 3.6 applied to $w' \ge w''$ and p, δ gives the bound

$$A(\Delta, w') \le A(\Delta + \delta, w'') + p,$$
$$B(\Delta, w') \le B(\Delta + \delta, w'') + \frac{(4/p)^{w'}}{\delta(1-\Delta)\kappa^{w''}}.$$

We apply this iteratively for some widths $w_0, \dots, w_r$. Set $w_0 = w$ and $w_{i+1} = \lceil (1-\varepsilon) w_i \rceil$ for some ε as long as $w_i > w^*$ for some w^*. In particular, we need $w^* \ge 1/\varepsilon$ to ensure $w_{i+1} < w_i$ and we will optimize ε, w^* later. The number of steps is thus $r \le (u \log w)/\varepsilon$ for some constant $u > 0$. Let $p_1, \dots, p_r$ and $\delta_1, \dots, \delta_r$ be the values we use for p, δ at each iteration. To simplify the notation, let $\Delta_i = \delta_1 + \cdots + \delta_i$ and $\Delta_0 = 0$. Furthermore, define

$$\gamma_i = \frac{(4/p_i)^{w_{i-1}}}{\kappa^{w_i}}.$$

Then for $i = 1, \dots, r$, we have

$$A(\Delta_{i-1}, w_{i-1}) \le A(\Delta_i, w_i) + p_i,$$
$$B(\Delta_{i-1}, w_{i-1}) \le B(\Delta_i, w_i) + \frac{\gamma_i}{\delta_i(1-\Delta_{i-1})}.$$

Set $p_i = \alpha/(2r)$ and $\delta_i = \sqrt{\gamma_i}$. We will select the parameters so that $\Delta_i \le 1/2$ for all i. Thus

$$A(0, w) \le A(\Delta_r, w_r) + \alpha/2 \le A(1/2, w^*) + \alpha/2,$$
$$B(0, w) \le B(\Delta_r, w_r) + 2\Delta_r \le B(1/2, w^*) + 2\Delta_r.$$

Plugging in the values for δ_i, we compute the sum

$$\Delta_r = \sum_{i=1}^{r} \delta_i \le \sum_{i=1}^{r} \sqrt{\frac{(4/p)^{w_{i-1}}}{\kappa^{(1-\varepsilon)w_{i-1}}}}$$
$$\le \sum_{k \ge w^*} \left(\frac{u \log w}{\varepsilon\alpha\kappa^{1-\varepsilon}}\right)^{k/2} \le 2\left(\frac{u \log w}{\varepsilon\alpha\kappa^{1-\varepsilon}}\right)^{w^*/2},$$

assuming $\kappa^{1-\varepsilon} = \Omega((\log w)/(\varepsilon\alpha))$. More precisely, if we take κ so that

$$\kappa^{1-\varepsilon} = \frac{K \cdot u \log w}{\varepsilon\alpha}, \qquad K \ge 4,$$

then $\Delta_r \le 2K^{-w^*/2}$.

Next, we apply Lemma 3.9 to bound $A(1/2, w^*) \le \alpha/2$ and $B(1/2, w^*) \le \beta/2$. Observe that $(1/2; \kappa^{-1}, \dots, \kappa^{-w^*})$-bounded set systems are also $(1; (\kappa/2)^{-1}, \dots, (\kappa/2)^{-w^*})$-bounded, in which case we can apply Lemma 3.9 and obtain that we need

$$\kappa \ge \Omega((1 + \log(1/\beta)) \cdot w^*/\alpha).$$

Let us now put the bounds together. We still have the freedom to choose $\varepsilon > 0$ and $w^* \ge 1/\varepsilon$. To obtain $A(0, w) \le \alpha, B(0, w) \le \beta$, we also need $\Delta_r \le \beta/2 < 1/2$. Thus all the constraints are:

(1) $w^* \ge 1/\varepsilon$;
(2) $\kappa^{1-\varepsilon} = (K \cdot u \log w)/(\varepsilon\alpha)$ for some constant $K \ge 4$;
(3) $\kappa \ge \Omega((1 + \log(1/\beta)) \cdot w^*/\alpha)$;
(4) $2K^{-w^*/2} \le \beta/2 \Longleftarrow w^* \ge \Omega(\log(1/\beta)/\log K)$.

Set $\varepsilon = 1/\log\log w$ and $w^* = c \cdot \max\{\log\log w, \log(1/\beta)\}$ for some $c \ge 1$. Then we obtain that the result holds whenever

$$\kappa = \Omega\left(\max\left\{\left(\frac{1}{\alpha}\right)^{1+2/\log\log w} \log w \log\log w, \frac{1}{\alpha}(\log(1/\beta))^2, \frac{1}{\alpha}\log(1/\beta)\log\log w\right\}\right).$$

In particular, it suffices to set $\kappa = \log w \cdot (\log\log w \cdot \log(1/\beta)/\alpha)^{O(1)}$.

ACKNOWLEDGMENTS

We thank Noga Alon, Matthew Wales, Mohammadmahdi Jahanara, and anonymous reviewers for helpful suggestions on an earlier version of this paper. We also thank Andrew Thomason, Gil Kalai, and Peter Frankl for pointing us to relevant references.

REFERENCES

[1] Noga Alon, Mauricio Karchmer, and Avi Wigderson. 1990. Linear Circuits over GF(2). *SIAM J. Comput.* 19, 6 (1990), 1064–1067.
[2] Noga Alon, Amir Shpilka, and Christopher Umans. 2013. On sunflowers and matrix multiplication. *Computational Complexity* 22, 2 (2013), 219–243. https://doi.org/10.1007/s00037-013-0060-1
[3] Noga Alon and Joel H Spencer. 2004. *The probabilistic method.* John Wiley & Sons.
[4] Nikhil Balaji, Samir Datta, Raghav Kulkarni, and Supartha Podder. 2016. Graph Properties in Node-Query Setting: Effect of Breaking Symmetry. In *41st International Symposium on Mathematical Foundations of Computer Science (MFCS 2016).* Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.
[5] Omer Berkman, Yossi Matias, and Prabhakar Ragde. 1998. Triply-logarithmic parallel upper and lower bounds for minimum and range minima over small domains. *Journal of Algorithms* 28, 2 (1998), 197–215.
[6] Bruno Pasqualotto Cavalar, Mrinal Kumar, and Benjamin Rossman. 2020. Monotone Circuit Lower Bounds from Robust Sunflowers.
[7] Marek Cygan, Fedor V. Fomin, Lukasz Kowalik, Daniel Lokshtanov, Dániel Marx, Marcin Pilipczuk, Michal Pilipczuk, and Saket Saurabh. 2015. *Parameterized Algorithms.* Springer. https://doi.org/10.1007/978-3-319-21275-3
[8] Dana Dachman-Soled, Mukul Kulkarni, and Aria Shahverdi. 2019. Tight upper and lower bounds for leakage-resilient, locally decodable and updatable non-malleable codes. *Information and Computation* (2019).
[9] Holger Dell and Dániel Marx. 2012. Kernelization of packing problems. In *Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2012, Kyoto, Japan, January 17-19, 2012.* 68–81. https://doi.org/10.1137/1.9781611973099.6
[10] Michel Deza and Peter Frankl. 1981. Every large set of equidistant (0, +1, −1)-vectors forms a sunflower. *Combinatorica* 1, 3 (1981), 225–231.
[11] Irit Dinur and Samuel Safra. 2005. On the hardness of approximating minimum vertex cover. *Annals of mathematics* (2005), 439–485.
[12] Rodney G Downey and Michael Ralph Fellows. 2012. *Parameterized complexity.* Springer Science & Business Media.

[13] Paul Erdős and Richard Rado. 1960. Intersection theorems for systems of sets. *Journal of the London Mathematical Society* 35, 1 (1960), 85–90.

[14] Jörg Flum and Martin Grohe. 2006. *Parameterized Complexity Theory*. Springer. https://doi.org/10.1007/3-540-29953-X

[15] Gudmund Skovbjerg Frandsen, Peter Bro Miltersen, and Sven Skyum. 1997. Dynamic word problems. *J. ACM* 44, 2 (1997), 257–271.

[16] Keith Frankston, Jeff Kahn, Bhargav Narayanan, and Jinyoung Park. 2019. Thresholds Versus Fractional Expectation-Thresholds. *arXiv preprint arXiv:1910.13433* (2019).

[17] Junichiro Fukuyama. 2018. Improved Bound on Sets Including No Sunflower with Three Petals. *arXiv preprint arXiv:1809.10318* (2018).

[18] Anna Gál and Peter Bro Miltersen. 2007. The cell probe complexity of succinct data structures. *Theoretical Computer Science* 379, 3 (2007), 405–417.

[19] Craig Gentry, Zulfikar Ramzan, and David P Woodruff. 2006. Explicit exclusive set systems with applications to broadcast encryption. In *2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*. IEEE, 27–38.

[20] Parikshit Gopalan, Raghu Meka, and Omer Reingold. 2013. DNF sparsification and a faster deterministic counting algorithm. *Computational Complexity* 22, 2 (2013), 275–310.

[21] Vince Grolmusz and Prabhakar Ragde. 1990. Incomparability in parallel computation. *Discrete Applied Mathematics* 29, 1 (1990), 63–78. https://doi.org/10.1016/0166-218X(90)90082-N

[22] Johan Håstad. 1987. *Computational limitations of small-depth circuits*. MIT Press, Cambridge, MA, USA.

[23] Ishay Haviv and Ning Xie. 2017. Sunflowers and testing triangle-freeness of functions. *computational complexity* 26, 2 (2017), 497–530.

[24] Bart MP Jansen and Dániel Marx. 2015. Characterizing the easy-to-find subgraphs from the viewpoint of polynomial-time algorithms, kernels, and Turing kernels. In *Proceedings of the twenty-sixth annual ACM-SIAM symposium on Discrete algorithms*. Society for Industrial and Applied Mathematics, 616–629.

[25] Stasys Jukna. 2010. Representing (0, 1)-matrices by boolean circuits. *Discrete Mathematics* 310, 1 (2010), 184–187. https://doi.org/10.1016/j.disc.2009.07.011

[26] Ilan Komargodski, Moni Naor, and Eylon Yogev. 2019. White-box vs. black-box complexity of search problems: Ramsey and graph property testing. *Journal of the ACM (JACM)* 66, 5 (2019), 34.

[27] AV Kostochka. 1997. A bound of the cardinality of families not containing Δ-systems. In *The Mathematics of Paul Erdős II*. Springer, 229–235.

[28] Xin Li, Shachar Lovett, and Jiapeng Zhang. 2018. Sunflowers and quasi-sunflowers from randomness extractors. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

[29] Shachar Lovett, Noam Solomon, and Jiapeng Zhang. 2019. From DNF Compression to Sunflower Theorems via Regularity. In *34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA*. 5:1–5:14. https://doi.org/10.4230/LIPIcs.CCC.2019.5

[30] Shachar Lovett, Kewen Wu, and Jiapeng Zhang. 2019. Decision list compression by mild random restrictions. *Electronic Colloquium on Computational Complexity (ECCC)* 26 (2019), 137. https://eccc.weizmann.ac.il/report/2019/137

[31] Shachar Lovett and Jiapeng Zhang. 2019. DNF sparsification beyond sunflowers. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*. ACM, 454–460.

[32] Michael Luby and Jessica Staddon. 1998. Combinatorial bounds for broadcast encryption. *Advances in CryptologyâĂŤEUROCRYPT'98* (1998), 512–526.

[33] Dániel Marx. 2005. Parameterized complexity of constraint satisfaction problems. *Computational Complexity* 14, 2 (2005), 153–183.

[34] Christian Worm Mortensen, Rasmus Pagh, and Mihai PÇŐtraçcu. 2005. On dynamic range reporting in one dimension. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*. ACM, 104–111.

[35] Dalit Naor, Moni Naor, and Jeff Lotspiech. 2001. Revocation and tracing schemes for stateless receivers. In *Annual International Cryptology Conference*. Springer, 41–62.

[36] Sivaramakrishnan Natarajan Ramamoorthy and Anup Rao. 2018. Lower bounds on non-adaptive data structures maintaining sets of numbers, from sunflowers. In *33rd Computational Complexity Conference (CCC 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

[37] Mohammad Ziaur Rahman. 2007. *Data Structuring Problems in the Bit Probe Model*. Master's thesis. University of Waterloo.

[38] Anup Rao. 2019. Coding for Sunflowers. *CoRR* abs/1909.04774 (2019). arXiv:1909.04774 http://arxiv.org/abs/1909.04774

[39] Alexander A Razborov. 1995. Bounded arithmetic and lower bounds in Boolean complexity. In *Feasible Mathematics II*. Springer, 344–386.

[40] Benjamin Rossman. 2014. The Monotone Complexity of k-Clique on Random Graphs. *SIAM J. Comput.* 43, 1 (2014), 256–279. https://doi.org/10.1137/110839059