On Sunflowers and Matrix Multiplication

Noga Alon [*] Amir Shpilka [†] Christopher Umans [‡]

Abstract

We present several variants of the sunflower conjecture of Erdős and Rado [ER60] and discuss the relations among them.

We then show that two of these conjectures (if true) imply negative answers to questions of Coppersmith and Winograd [CW90] and Cohn et al [CKSU05] regarding possible approaches for obtaining fast matrix multiplication algorithms. Specifically, we show that the Erdős-Rado sunflower conjecture (if true) implies a negative answer to the "no three disjoint equivoluminous subsets" question of Coppersmith and Winograd [CW90]; we also formulate a "multicolored" sunflower conjecture in $\mathbb{Z}_3^n$ and show that (if true) it implies a negative answer to the "strong USP" conjecture of [CKSU05] (although it does not seem to impact a second conjecture in [CKSU05] or the viability of the general group-theoretic approach). A surprising consequence of our results is that the Coppersmith-Winograd conjecture actually implies the Cohn et al. conjecture.

The multicolored sunflower conjecture in $\mathbb{Z}_3^n$ is a strengthening of the well-known (ordinary) sunflower conjecture in $\mathbb{Z}_3^n$, and we show via our connection that a construction from [CKSU05] yields a lower bound of $(2.51\ldots)^n$ on the size of the largest *multicolored* 3-sunflower-free set, which beats the current best known lower bound of $(2.21\ldots)^n$ [Edel04] on the size of the largest 3-sunflower-free set in $\mathbb{Z}_3^n$.

1 Introduction

Sunflowers. A *k-sunflower* (also called a Δ-*system* of size k) is a collection of k sets, from some universe U, that have the same pairwise intersections. This notion was first introduced in [ER60] and proved itself to be a very useful tool in combinatorics, number theory and computer science ever since. See, e.g., [Fu91], [Ju01], [AP01].

A basic problem concerning sunflowers is how many sets do we need in order to guarantee the existence of a k-sunflower. Erdős and Rado proved the following bound [ER60, ER69].

[*] Sackler School of Mathematics and Blavatnik School of Computer Science, Tel Aviv University, Tel Aviv 69978, Israel. Email: nogaa@tau.ac.il. Research supported in part by an ERC Advanced Grant.

[†] Faculty of Computer Science, Technion-Israel Institute of Technology, Haifa, Israel. Email: shpilka@cs.technion.ac.il. The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement number 257575.

[‡] Computing and Mathematical Sciences, California Institute of Technology, Pasadena, CA 91125. Email: umans@cs.caltech.edu. Research supported in part by NSF CCF-0830787.

Theorem 1.1 (Erdős and Rado [ER60]) *Let $\mathcal{F}$ be an arbitrary family of sets of size s from some universe U. If $|\mathcal{F}| > (k-1)^s \cdot s!$ then $\mathcal{F}$ contains a k-sunflower.*

They conjectured that actually many fewer sets are needed.

Conjecture 1 (Classical sunflower conjecture [ER60]) *For every $k > 0$ there exists a constant c_k such that the following holds. Let $\mathcal{F}$ be an arbitrary family of sets of size s from some universe U. If $|\mathcal{F}| \geq c_k^s$ then $\mathcal{F}$ contains a k-sunflower.*

This (and in particular the case $k = 3$) is one of the most well known open problems in combinatorics and despite a lot of attention it is still open today (see e.g. [Erd71, Erd75, Erd81]).

This conjecture has applications in combinatorial number theory and the study of Turán type problems in extremal graph theory ([Fu91]), as well as in other areas in combinatorics including the investigation of explicit constructions of Ramsey graphs ([AP01]). A close variant has been applied in Circuit Complexity ([Ju01], see also [Ra85], [AB87]).

Matrix multiplication. A fundamental algorithmic problem in computer science asks to compute the product of two given $n \times n$ matrices. This problem received a lot of attention since the seminal work of Strassen [Str69] that showed that one can do better than the simple row-column multiplication. The best known result is due to Coppersmith and Winograd that gave an $O(n^{2.376\ldots})$ time algorithm for multiplying two $n \times n$ matrices [CW90]. It is widely believed by experts that one should be able to multiply $n \times n$ matrices in time $O(n^{2+\epsilon})$, for every $\epsilon > 0$ (see e.g., [Gat88, BCS97]). It is a major open problem to achieve such an algorithm (which we term fast matrix multiplication).

In their paper, Coppersmith and Winograd proposed an approach towards achieving fast matrix multiplication. They showed that the existence of an Abelian group and a subset of it that satisfy certain conditions, imply that their techniques can yield an $O(n^{2+\epsilon})$ time algorithm. As we shall later see, if Conjecture 1 is true then no such group and subset exist.

A new approach for matrix multiplication that is based on group representation theory was suggested by Cohn and Umans [CU03]. In a subsequent work [CKSU05], Cohn et al. gave several algorithms based on the framework of [CU03], and were even able to match the result of [CW90]. Similarly to Coppersmith and Winograd, Cohn et al. formulated two questions regarding the existence of certain combinatorial structures that, if true, would yield fast matrix-multiplication algorithms. We formulate a variant of the sunflower conjecture (Conjecture 6) and prove that it contradicts one of their questions, regarding the existence of "strong Uniquely Solvable Puzzles." Thus any construction of strong Uniquely-Solvable Puzzles that would yield an exponent 2 algorithm for matrix multiplication must disprove this variant of the sunflower conjecture, which helps explain the difficulty of the problem.

We stress though, that this does not rule out the possibility of obtaining fast matrix multiplication algorithms using the Cohn-Umans framework. In particular, in [CKSU05] Cohn et al. propose a second direction that seems not to contradict the variants of the sunflower conjecture that are considered here.

Organization. We organize the paper as follows. In Section 2 we discuss different sunflower conjectures and give the relations among them. In Section 3 we present the questions raised in [CW90, CKSU05] and show their relation to sunflowers.

Notations. For an integer m we denote by $\mathbb{Z}_m = \{0, \ldots, m-1\}$ the additive group modulo m. $[n]$ stands for the set $[n] = \{1, \ldots, n\}$. All logarithms are taken in base 2. We will often use *direct products* of families of sets. For families $\mathcal{F}_1 \subset \mathbb{Z}_m^{n_1}$ and $\mathcal{F}_2 \subset \mathbb{Z}_m^{n_2}$, we define their direct product to be the family $\mathcal{F}_1 \times \mathcal{F}_2 = \{u \circ v \mid u \in \mathcal{F}_1 \text{ and } v \in \mathcal{F}_2\}$, where $u \circ v$ is the concatenation of u and v, over $\mathbb{Z}_m^{n_1+n_2}$. When each $\mathcal{F}_i$ is a family of subsets from some universe U_i, we define the direct product analogously, over the disjoint union $U_1 \sqcup U_2$.

2 Sunflower conjectures

Definition 2.1 *We say that k subsets $A_1, \ldots, A_k$, of a universe U, form a k-*sunflower *if $\forall i \neq j$ $A_i \cap A_j = \cap_{i=1}^k A_i$.*

Conjecture 1 states that for every k there is an integer c_k such that any c_k^s sets of size s contain a k-sunflower. The conjecture is open even for $k = 3$, which is the case that we are most interested in, in this paper. This case is also the main one studied in most existing papers on the conjecture, and it is believed that any proof of the conjecture for $k = 3$ is likely to provide a proof of the general case as well. Currently the best known result is given in the following theorem of Kostochka, improving an earlier estimate of [Spe77].

Theorem 2.2 (Kostochka [Ko97]) *There exists a constant c such that every family of s-sets of size at least $cs! \cdot (\frac{\log\log\log s}{\log\log s})^s$ contains a 3-sunflower.*

The following conjecture of Erdős and Szemerédi [ES78] concerns 3-sunflowers inside $[n]$.

Conjecture 2 (Sunflower conjecture in $\{0,1\}^n$ [ES78]) *There exists $\epsilon > 0$ such that any family $\mathcal{F}$ of subsets of $[n]$ $(n \geq 2)$ of size $|\mathcal{F}| \geq 2^{(1-\epsilon)\cdot n}$ contains a 3-sunflower.*

Note the difference between Conjectures 1 and 2. While Conjecture 1 concerns s-sets from an unbounded universe, Conjecture 2 does not restrict the sets to be of the same size, and instead demands that they all come from an n element set.

An interesting fact is that Conjecture 1 implies Conjecture 2. This was proved in [ES78] (see also [DEGKM97] for a somewhat sharper estimate). For completeness, we include a short proof.

Theorem 2.3 ([ES78]) *Assume that for $k = 3$ there exists a constant c such that every family of s-sets of size at least c^s contains a 3-sunflower. Set $\epsilon = 1/4c$. Then any family $\mathcal{F}$ of subsets of $[n]$ of size $|\mathcal{F}| \geq 2^{(1-\epsilon)n}$ contains a 3-sunflower.*

Proof Recall that $\sum_{i=0}^{(\frac{1}{2}-\delta)n}\binom{n}{i} = 2^{(1+o(1))H(\frac{1}{2}-\delta)\cdot n}$, where $H(x) = -x\log(x) - (1-x)\log(1-x)$ is the entropy function. As $H(\frac{1}{2}-\delta) < 1-\delta^2$, for δ small enough, we get that for $\delta = \sqrt{2\epsilon}$, $\mathcal{F}$ must contain at least $\frac{1}{4\delta n}2^{(1-\epsilon)\cdot n}$ sets of size s for some $s \in [(\frac{1}{2}-\delta)\cdot n, (\frac{1}{2}+\delta)\cdot n]$. From now on we shall only consider those sets of size exactly s in $\mathcal{F}$.

Let $\alpha > 0$ be some small number to be determined later, such that $\alpha \cdot n$ is an integer. As each s-set contains exactly $\binom{s}{s-\alpha n}$ subsets of size $s-\alpha n$, and there are $\binom{n}{s-\alpha n}$ such sets, one $(s-\alpha n)$-set belongs to at least

$$\begin{aligned} \frac{1}{4\delta n}2^{(1-\epsilon)\cdot n}\cdot\frac{\binom{s}{s-\alpha n}}{\binom{n}{s-\alpha n}} &= \frac{1}{4\delta n}2^{(1-\epsilon)\cdot n}\cdot\frac{\binom{n+\alpha n}{\alpha n}}{\binom{n+\alpha n}{s}} > \frac{1}{4\delta n}2^{(1-\epsilon)\cdot n}\cdot\frac{\binom{n+\alpha n}{\alpha n}}{2^{n+\alpha n}} \\ &= 2^{H(\frac{\alpha}{1+\alpha})\cdot(1+\alpha)n-\alpha n-\epsilon n-o(n)} > 2^{n\left(\alpha\log(\frac{1+\alpha}{\alpha})-\alpha-\epsilon\right)} \end{aligned} \qquad (1)$$

s-sets in $\mathcal{F}$. Let $\alpha = 1/4c$ and $\epsilon \leq \alpha$. From (1) it follows that, for some $(s-\alpha n)$-set A, the number of s-sets in $\mathcal{F}$ that contain A is larger than

$$2^{n\left(\alpha\log(\frac{1+\alpha}{\alpha})-\alpha-\epsilon\right)} \geq 2^{n\alpha\log c} = c^{\alpha n}\ .$$

By the choice of c, it follows that if we remove the set A from all those sets then three of them form a sunflower (indeed, after removing A, we get a collection of more than $c^{\alpha n}$ sets of size αn). In particular, a sunflower exists in $\mathcal{F}$. □

The same proof idea can be used to show a strong consequence if Conjecture 2 is false, that will be useful in the proof of Theorem 2.7.

Theorem 2.4 *If Conjecture 2 is false, then the following holds for every $\epsilon > 0$. For infinitely many n, for all integers $2 \leq c < 1/\sqrt{\epsilon}$, there are families $\mathcal{F}$ of n-subsets of $[cn]$ of cardinality $\binom{cn}{n}^{1-\epsilon}$, containing no 3-sunflower.*

Proof Let $\mathcal{F}$ be a family of $2^{(1-\epsilon)m}$ subsets of $[m]$ that contain no 3-sunflowers. Then repeating the first part of the proof of Theorem 2.3, we can find a family $\mathcal{F}' \subseteq \mathcal{F}$ of at least $\frac{1}{4\sqrt{2\epsilon}m}2^{(1-\epsilon)m}$ s-subsets of $[m]$ for some $s \in [(1/2-\sqrt{2\epsilon})m, (1/2+\sqrt{2\epsilon})m]$. If m is odd, add an element to the universe and set $m' = m+1$; otherwise set $m' = m$. If $s = m'/2 + \ell$ for integer $\ell > 0$, then add 2ℓ fresh elements to the universe $[m']$. If $s = m'/2 - \ell$ for integer $\ell > 0$, then add 2ℓ fresh elements to the universe $[m']$ and to every subsets in $\mathcal{F}'$ to obtain a 3-sunflower-free family of $(m'/2+\ell)$-subsets of $[m'+2\ell]$. In both cases, since $\ell \leq \sqrt{2\epsilon}m$, the cardinality is at least

$$\frac{1}{4\sqrt{2\epsilon}m}2^{(1-\epsilon)m} \geq \frac{1}{8\sqrt{2\epsilon}m}2^{(1-\epsilon)m'} \geq \frac{1}{8\sqrt{2\epsilon}m}2^{\frac{1-\epsilon}{1+2\sqrt{2\epsilon}}(m'+2\ell)}.$$

Assuming Conjecture 2 is false, we have families $\mathcal{F}$ of $2^{(1-\epsilon)m}$ subsets of $[m]$ that contain no 3-sunflowers, for arbitrarily small $\epsilon > 0$, and infinitely many m. Applying the above transformation, we have that for every $\epsilon > 0$, and infinitely many n, there are families of n-subsets of $[2n]$ of cardinality $2^{(1-\epsilon)2n} \geq \binom{2n}{n}^{1-\epsilon}$. This takes care of the case $c = 2$.

Now, we turn to the cases $2 < c < 1/\epsilon$. By taking the $(c-1)$-fold direct product of the $c = 2$ construction, we obtain families of $(c-1)n$-subsets of $[2(c-1)n]$ of cardinality at least

$2^{2(c-1)n(1-\epsilon)} \geq \binom{2(c-1)n}{(c-1)n}^{1-\epsilon}$. Consider such a 3-sunflower-free family (note that a direct product of sunflower-free families is also sunflower-free). Set $r = (c-2)n$. The number of r-subsets of $[2(c-1)n]$ is

$$\binom{2(c-1)n}{r} = \frac{\binom{2(c-1)n}{(c-1)n}\binom{(c-1)n}{r}}{\binom{2(c-1)n-r}{(c-1)n-r}}.$$

The number of r-subsets of each set in the family is $\binom{(c-1)n}{r}$. Thus, there is some r-set contained in at least

$$\binom{2(c-1)n}{(c-1)n}^{1-\epsilon} \cdot \frac{\binom{2(c-1)n-r}{(c-1)n-r}}{\binom{2(c-1)n}{(c-1)n}} \geq \frac{\binom{2(c-1)n-r}{(c-1)n-r}}{2^{2\epsilon(c-1)n}}.$$

subsets in the family. Remove this r-set from these subsets and the universe. Since $2(c-1)n - r = cn$ and $(c-1)n - r = n$, the resulting family consists of n-subset of $[cn]$ that are 3-sunflower-free, and it has cardinality at least

$$\frac{\binom{cn}{n}}{2^{2\epsilon(c-1)n}} \geq \frac{\binom{cn}{n}^{1-2\sqrt{\epsilon}} c^{2\sqrt{\epsilon}n}}{2^{2\epsilon(c-1)n}} \geq \binom{cn}{n}^{1-2\sqrt{\epsilon}},$$

using the fact that $\binom{cn}{n} \geq c^n$, and the requirement that $2 \leq c < 1/\sqrt{\epsilon}$. As $\epsilon > 0$ was arbitrary, we are done. □

In order to relate sunflowers to the question of Cohn et al. we need to consider the following variant of sunflowers.

Definition 2.5 (Sunflowers in $\mathbb{Z}_D^n$) *We say that k vectors $v_1, \ldots, v_k \in \mathbb{Z}_D^n$ form a k-sunflower if for every coordinate $i \in [n]$ it holds that either $(v_1)_i = \ldots = (v_k)_i$ or they all differ on that coordinate.*

Note that this definition generalizes the notion of sunflower if we identify each subset of the universe U with its characteristic vector.

Conjecture 3 (Sunflower conjecture in $\mathbb{Z}_D^n$) *For every k there is an absolute constant b_k so that for every D and every n any set of at least b_k^n vectors in $\mathbb{Z}_D^n$ contains a k-sunflower.*

While this conjecture seems different from the classical sunflower conjecture, it turns out that they are equivalent.

Theorem 2.6 *If Conjecture 1 holds for c_k then Conjecture 3 is true for $b_k = c_k$. Similarly, if Conjecture 3 holds for b_k, then Conjecture 1 is true with $c_k = e \cdot b_k$.*

Proof Conjecture 1 ⇒ Conjecture 3: Let $U = \mathbb{Z}$ and denote by $p_1, \ldots, p_n$ the first n prime numbers. Given $v \in \mathbb{Z}_D^n$ define $S_v = \{p_1^{1+v_1}, \ldots, p_n^{1+v_n}\}$. Clearly S_v is an n-set. It is not hard to see that a collection $\mathcal{F} \subseteq \mathbb{Z}_D^n$ contains a k-sunflower if and only if the corresponding family $S_{\mathcal{F}} = \{S_v \mid v \in \mathcal{F}\}$ contains a k-sunflower.

Conjecture 3 $\Rightarrow$ Conjecture 1: Given a family $\mathcal{F}$ of c^s subsets of U we shall define a corresponding family inside $\mathbb{Z}_D^s$, for some large D. Indeed, we can assume w.l.o.g. that $|U| \leq s \cdot c^s$. For convenience assume that $U = [D]$ for $D \leq s \cdot c^s$. Pick a map from $[D]$ to $[s]$ uniformly at random from all such maps. For a given s-set $A \subset [D]$, the probability that A was mapped injectively to $[s]$ is exactly $s!/s^s > e^{-s}$. Thus, there exists a map $f : [D] \to [s]$, that is $1-1$ on at least $(c/e)^s$ of the sets in $\mathcal{F}$. Denote those sets by $\tilde{\mathcal{F}}$ and consider any such set A. Define the vector $v_A = (v_1, \ldots, v_s)$ where $v_i = f^{-1}(i) \cap A$. Namely, the ith coordinate of v is the unique element of A that was mapped to i by f. Denote the new family by $v_{\mathcal{F}}$. It is not hard to see that $\tilde{\mathcal{F}}$ contains a k-sunflower if and only if $v_{\mathcal{F}}$ does. As $|v_{\mathcal{F}}| = |\tilde{\mathcal{F}}| \geq (c/e)^s = b^s$, where $b = c/e$, the result follows. □

The following is a weaker version of Conjecture 3, for the special case $k = 3$.

Conjecture 4 (Weak sunflower conjecture in $\mathbb{Z}_D^n$) *There is an $\epsilon > 0$ so that for $D > D_0$ and $n > n_0$, any set of at least $D^{(1-\epsilon)n}$ vectors in Z_D^n contains a 3-sunflower.*

The main difference from Conjecture 3 is that we allow the number of sets to scale with D. It is clear that Conjecture 3 immediately implies Conjecture 4. Next we show that Conjecture 4 is in fact equivalent to Conjecture 2.

Theorem 2.7 *If Conjecture 2 holds for ϵ_0 then Conjecture 4 holds for $\epsilon = \epsilon_0/2$, $D_0 \geq 2^{\frac{12}{\epsilon_0^2}}$ and $n > n_0$. If Conjecture 4 holds for ϵ_0 and $D_0 \geq 3$ and $n > n_0$ then Conjecture 2 holds for some $\epsilon_0' > 0$.*

Proof Conjecture 2 $\Rightarrow$ Conjecture 4: Let d be such that $\binom{d}{d/2} \geq D$ (by Stirling's approximation, $d = \log D + \frac{1}{2}\log\log D + 3$ suffices). Pick an arbitrary 1-1 map f from $[D]$ to subsets of size $d/2$ in $\{0,1\}^d$. Given a family $\mathcal{F} \subset \mathbb{Z}_D^n$ map every vector $v \in \mathcal{F}$ to $v' \in \{0,1\}^{dn}$ in the natural way. I.e. $v' = f(v_1) \circ f(v_2) \circ \cdots \circ f(v_n)$, where $\circ$ stands for concatenation. Call the resulting family $\mathcal{F}'$. It is clear that if v', u', w' form a 3-sunflower in $\{0,1\}^{dn}$ then v, u, w form a 3-sunflower in $\mathbb{Z}_D^n$ (the converse is not necessarily true). From our choice of parameters it follows that $|\mathcal{F}'| = |\mathcal{F}| \geq D^{(1-\epsilon)n} \geq 2^{(1-\epsilon_0)dn}$. Hence, $\mathcal{F}'$ contains a 3-sunflower and therefore so does $\mathcal{F}$.

Conjecture 4 $\Rightarrow$ Conjecture 2: Assume that Conjecture 2 is false. By Theorem 2.4, we can choose $\epsilon < \min(\epsilon_0/2, 1/D_0^2)$ and then for infinitely many n, for each $2 \leq c \leq D_0$ there is a family $\mathcal{F}_c$ of at least $\binom{cn}{n}^{1-\epsilon_0/2}$ n-subsets of $[cn]$. We now describe a family of vectors in $\mathbb{Z}_{D_0}^{D_0 n}$. We use the phrases "0-set," "1-set," etc... to refer to the coordinates of a given vector that have 0s, 1s, etc... Our vectors have as their 0-sets the subsets in family $\mathcal{F}_{D_0}$. For each 0-set, we have vectors whose 1-sets (which are subsets of the remaining $(D_0-1)n$ coordinates) are given by family $\mathcal{F}_{D_0-1}$. Then for each pattern of 0s and 1s, we have vectors whose 2-sets (which are subsets of the remaining $(D_0-2)n$ coordinates) are given by family $\mathcal{F}_{D_0-2}$, and so on, until we define the (D_0-2)-sets using family $\mathcal{F}_2$. The remaining n coordinates of each vector are then set to $D_0 - 1$. It is clear that if three vectors u, v, w in this family form a 3-sunflower, then their 0-sets coincide (since $\mathcal{F}_{D_0}$ is 3-sunflower-free), and then their 1-sets coincide (since $\mathcal{F}_{D_0-1}$

is 3-sunflower-free), and so on, until we conclude that $u = v = w$. Thus our family in $\mathbb{Z}_{D_0}^{D_0 n}$ is 3-sunflower free, and it has cardinality at least

$$\begin{aligned}\left(\binom{D_0 n}{n}\binom{(D_0-1)n}{n}\binom{(D_0-2)n}{n}\cdots\binom{2n}{n}\right)^{1-\epsilon_0/2} &= \binom{D_0 n}{n, n, n, \cdots, n}^{1-\epsilon_0/2} \\ &\geq^{(*)} D_0^{D_0 n(1-o(1))(1-\epsilon_0/2)} \geq D_0^{(1-\epsilon_0)D_0 n},\end{aligned}$$

where $(*)$ follows easily from Stirling's theorem. □

The assertion of Conjecture 4 may well hold for small values of D as well. In particular, the case $D = 3$ attracted a considerable amount of attention as in this case a 3-sunflower in the group $\mathbb{Z}_3^n$ is equivalent to a 3-term arithmetic progression in this group.

Conjecture 5 (Weak sunflower conjecture in $\mathbb{Z}_3^n$) *There is an $\epsilon > 0$ so that for $n > n_0$, any set of at least $3^{(1-\epsilon)n}$ vectors in Z_3^n contains a 3-sunflower.*

An obvious modification of the previous proof (replacing any symbol of $[D]$ by its base-3 representation) shows that Conjecture 5 implies Conjecture 4. The best known upper bound for the cardinality of a subset of Z_3^n that contains no 3-sunflower is the recent $O(3^n/n^{1+\epsilon})$ bound, for some small $\epsilon > 0$, of [BK11] that improves upon the previous $2 \cdot 3^n/n$ bound of [Me95]. The best known lower bound is $(2.217\ldots)^n$ [Edel04].

It is natural to guess that Conjecture 5 is true when it is seen as a variant of Conjecture 4. On the other hand, one might guess that Conjecture 5 is false when it is viewed as a variant of the assertion that sets of size $D^{(1-\epsilon)n}$ in Z_D^n have a 3-term arithmetic progression, because the latter statement is false for large D. We include a simple construction, due to Salem and Spencer [SS42]:

Theorem 2.8 (3-term arithmetic progression free sets in $\mathbb{Z}_D^n$ [SS42]) *For all $\epsilon > 0$, if $D > 2^{2/\epsilon}$ and n is sufficiently large, there is a set of $D^{(1-\epsilon)n}$ vectors in $\mathbb{Z}_D^n$ that contains no 3-term arithmetic progressions.*

Proof Set $d = \lfloor (D-1)/2 \rfloor$, and for simplicity assume $(d+1)|n$. Let $\mathcal{F}$ be the set of all vectors in $\mathbb{Z}_D^n$ with equal numbers of the elements $\{0, 1, 2, \ldots, d\}$. Then

$$|\mathcal{F}| = \binom{n}{n/(d+1), n/(d+1), \ldots, n/(d+1)} = (d+1)^{(1-o(1))n} \geq D^{(1-\epsilon/2-o(1))n} > D^{(1-\epsilon)n}$$

(if $(d+1) \nmid n$, we take vectors with a near-equal distribution, and the calculation is essentially unchanged).

Suppose we have $u, v, w \in \mathcal{F}$ for which $u + w = 2v$ (i.e., u, v, w form a 3-term arithmetic progression). Since all entries in u, v, w are at most d this equation holds in the integers as well. Then, consider the set I of coordinates i for which $v_i = d$. Since all entries in u, w are at most d, it must be that $u_i = w_i = d$ for all $i \in I$. But now we have accounted for all of the entries equal to d in all three vectors. The same argument then gives that all three vectors are $d - 1$

in exactly the same set of coordinates, etc... We conclude $u = v = w$. □

The last sunflower conjecture is a "multicolored" version of Conjecture 5. To formulate it, we will be discussing collections of ordered *triples* of vectors in $\mathbb{Z}_3^n$ (instead of collections of vectors in $\mathbb{Z}_3^n$). We say that such a triple (x, y, z) is an *ordered sunflower* if the set $\{x, y, z\}$ is a sunflower in $\mathbb{Z}_3^n$, and we say that two ordered sunflowers (x, y, z) and (a, b, c) are *disjoint* $x \neq a$, $y \neq b$, and $z \neq c$. We say that a collection of ordered triples contains a *multicolored sunflower* if it contains three triples, $(x^{(1)}, y^{(1)}, z^{(1)})$, $(x^{(2)}, y^{(2)}, z^{(2)})$, $(x^{(3)}, y^{(3)}, z^{(3)})$, not all equal, for which $\{x^{(1)}, y^{(2)}, z^{(3)}\}$ form a sunflower.

Conjecture 6 (multicolored sunflower conjecture in $\mathbb{Z}_3^n$) *There exists $\epsilon > 0$ so that for $n > n_0$, every collection $\mathcal{F} \subseteq \mathbb{Z}_3^n \times \mathbb{Z}_3^n \times \mathbb{Z}_3^n$ of at least $3^{(1-\epsilon)n}$ ordered sunflowers contains a multicolored sunflower.*

The requirement in Conjecture 6 that $\mathcal{F}$ be a collection of sunflowers (rather than an arbitrary collection of triples) is needed for non-triviality[1]. Note that if $\mathcal{F} \subseteq \mathbb{Z}_3^n$ is 3-sunflower-free, then $\{(x, x, x) : x \in \mathcal{F}\}$ is a collection of ordered sunflowers containing no multicolored sunflower. Thus Conjecture 6 implies Conjecture 5.

Figure 1 describes the connections between the different conjectures.

$$\begin{tikzcd}
& & \text{Conj. } 3 \arrow[r, Leftrightarrow, "\mathit{Thm.}\ 2.6"] \arrow[d, Rightarrow] & \text{Conj. } 1 \arrow[d, Rightarrow, "\mathit{Thm.}\ 2.3"] \\
\text{Conj. } 6 \arrow[r, Rightarrow] & \text{Conj. } 5 \arrow[r, Rightarrow] & \text{Conj. } 4 \arrow[r, Leftrightarrow, "\mathit{Thm.}\ 2.7"] & \text{Conj. } 2
\end{tikzcd}$$

Figure 1: Sunflower conjectures

3 Matrix multiplication

In [CW90] Coppersmith and Winograd gave the fastest algorithm known today for multiplying two $n \times n$ matrices. Their argument fell short of providing an $O(n^{2+\epsilon})$ time algorithm; however they proved that if a certain structure (that we define next) exists then their techniques can yield such an algorithm.

Definition 3.1 ([CW90]) *An Abelian group G (with at least two elements) and a subset S of G satisfy the* no three disjoint equivoluminous subsets *property if: whenever T_1, T_2 and T_3 are three disjoint subsets of S, not all empty, they cannot all have the same sum in G:*

$$\sum_{g \in T_1} g \neq \sum_{g \in T_2} g \quad \mathit{or} \quad \sum_{g \in T_2} g \neq \sum_{g \in T_3} g\ .$$

[1] Otherwise, e.g., the collection of ordered triples (x, y, z) with the first digit of $x = 0$, the first digit of $y = 0$, and the first digit of $z = 1$ contains no multicolored sunflower.

Coppersmith and Winograd showed that if "... we can find a sequence of pairs G, S with the no three disjoint equivoluminous subset property, such that $\log(|G|)/|S|$ approaches 0" then for every $\epsilon > 0$ there is an $O(n^{2+\epsilon})$ time fast matrix multiplication algorithm. However, the next claim, whose proof is very simple, shows that if Conjecture 2 is true then there is no such sequence.

Theorem 3.2 *If Conjecture 2 holds with ϵ_0 then if G, S have the no three disjoint equivoluminous subset property then $|S| \leq \log(|G|)/\epsilon_0$.*

Proof Given S, consider all its $2^{|S|}$ subsets. For each subset $T \subseteq S$, compute $\sigma(T) = \sum_{g \in T} g$. Clearly, there is some $g \in G$ such that at least $2^{|S|}/|G|$ subsets T satisfy $\sigma(T) = g$. Now, if $\log(|G|)/|S| < \epsilon_0$ then $2^{|S|}/|G| > 2^{(1-\epsilon_0)|S|}$. Therefore, in this case, Conjecture 2 implies the existence of a 3-sunflower T_1', T_2' and T_3' such that $\sigma(T_1') = \sigma(T_2') = \sigma(T_3')$. Let $T = T_1' \cap T_2'$. Set $T_i = T_i' \setminus T$. By our construction we have that the T_i's are disjoint and $\sigma(T_i) = g - \sigma(T)$. Hence, they violate the no three disjoint equivoluminous subsets property. Hence, we must have $|S| \leq \log(|G|)/\epsilon_0$ for the property to hold. □

We now turn to discussing a question that was formulated by Cohn et al. [CKSU05]. Denote by $\mathrm{Sym}(U)$ the group of permutations of a set U.

Definition 3.3 (Uniquely solvable puzzle [CKSU05]) *A uniquely solvable puzzle (USP) of width n is a subset $\mathcal{F} \subseteq \mathbb{Z}_3^n$ satisfying the following property: For all permutations $\pi_0, \pi_1, \pi_2 \in$ Sym($\mathcal{F}$), either $\pi_0 = \pi_1 = \pi_2$ or else there exist $u \in \mathcal{F}$ and $i \in [n]$ such that at least two of $(\pi_0(u))_i = 0$, $(\pi_1(u))_i = 1$, and $(\pi_2(u))_i = 2$ hold.*

The USP capacity is the largest constant C such that there exist USPs of size $(C - o(1))^n$ and width n for infinitely many values of n.

Quoting [CKSU05]: "The motivation for the name uniquely solvable puzzle is that a USP can be thought of as a jigsaw puzzle. The puzzle pieces are the sets $\{i : u_i = 0\}$, $\{i : u_i = 1\}$, and $\{i : u_i = 2\}$ with $u \in \mathcal{F}$, and the puzzle can be solved by permuting these types of pieces according to π_0, π_1, and π_2, respectively, and reassembling them without overlap into triples consisting of one piece of each of the three types. The definition requires that the puzzle must have a unique solution."

Cohn et al. observed that the USP capacity is at most $3/2^{2/3}$ and noticed that a construction of Coppersmith and Winograd implies that the capacity is at least $3/2^{2/3}$ [CW90]. They thus concluded that the USP capacity equals $3/2^{2/3}$. For the purpose of obtaining fast matrix multiplication algorithms, [CKSU05] require a structure that is more restrictive than USP, which they call a strong USP.

Definition 3.4 (Strong uniquely solvable puzzle [CKSU05]) *A strong USP is a USP $\mathcal{F} \subseteq \mathbb{Z}_3^n$ in which the defining property is strengthened as follows: For all permutations $\pi_0, \pi_1, \pi_2 \in$ Sym($\mathcal{F}$), either $\pi_0 = \pi_1 = \pi_2$ or else there exist $u \in \mathcal{F}$ and $i \in [n]$ such that exactly two of $(\pi_0(u))_i = 0$, $(\pi_1(u))_i = 1$, and $(\pi_2(u))_i = 2$ hold.*

The strong USP capacity is the largest constant C such that there exist strong USPs of size $(C - o(1))^n$ and width n for infinitely many values of n.

A variant of strong USPs that seems easier to reason about, but potentially harder to construct, is what [CKSU05] call a *local strong USP*. Expressing their definition slightly differently, we see the connection to sunflowers:

Definition 3.5 (local strong USP [CKSU05]) *A collection $\mathcal{F}$ of vectors in $\mathbb{Z}_3^n$ is a local strong USP if for every $u, v, w \in \mathcal{F}$, not all equal, the sets $\{i : u_i = 0\}$, $\{i : v_i = 1\}$, and $\{i : w_i = 2\}$ do not form a 3-sunflower. The local strong USP capacity is the largest constant C such that there exist local strong USPs of size $(C - o(1))^n$ in $\mathbb{Z}_3^n$ for infinitely many values of n.*

It is not hard to see that a local strong USP is a strong USP (Lemma 6.1 in [CKSU05]). More interestingly, we have the the strong USP capacity is achieved by local strong USPs (Proposition 6.3 in [CKSU05]). In particular, if the strong USP capacity is at least c, then for infinitely many n, there is a local strong USP $\mathcal{F} \subseteq \mathbb{Z}_3^n$ of size $(c - o(1))^n$. Cohn et al. conjectured that the strong USP capacity (and thus also the local strong USP capacity) is equal to the USP capacity. As shown in [CKSU05], this would imply an $O(n^{2+\epsilon})$ time algorithm for matrix multiplication.

Conjecture 7 (Conjecture 3.4 in [CKSU05]) *The strong USP capacity (and the local strong USP capacity) equals $3/2^{2/3}$.*

Next, we show that Conjecture 6 implies that Conjecture 7 is false. In the proof, it will be convenient if our local strong USPs have equal numbers of 0's, 1's, and 2's in each vector, and the next lemma shows this can be assumed without loss of generality.

Lemma 3.6 *If the strong USP capacity is at least c, then for infinitely many n, there is a local strong USP $\mathcal{F} \subseteq \mathbb{Z}_3^{3n}$ with each $v \in \mathcal{F}$ having equal numbers of 0's, 1's, and 2's, of cardinality at least $(c - o(1))^{3n}$.*

Proof We begin with local strong USP $U \subseteq \mathbb{Z}_3^m$ of cardinality at least $N = (c - o(1))^m$, which exists because the capacity is at least c. Now, form the strong USP $V \subseteq \mathbb{Z}_3^{mN}$ by taking all vectors that are the concatenation (in some order) of the N vectors of U. Each vector $v \in V$ now has the same distribution of 0's, 1's and 2's. It is easy to see that the local strong USP property is preserved when cyclically permuting $\mathbb{Z}_3$. The direct product of the three local strong USPs obtained from V by these three transformations is a local strong USP $\mathcal{F} \subseteq \mathbb{Z}_3^{3mN}$ with each $v \in \mathcal{F}$ having an equal number of 0's, 1's and 2's. Its cardinality is

$$(N!)^3 = \left(N^{N(1-o(1))}\right)^3 \geq \left((c - o(1))^{mN(1-o(1))}\right)^3 = (c - o(1))^{3mN}$$

for infinitely many values of m. □

Theorem 3.7 *If the strong USP capacity is at least c, then for infinitely many N, there exists a collection of at least $(2^{2/3}c - o(1))^N$ ordered sunflowers in $\mathbb{Z}_3^N \times \mathbb{Z}_3^N \times \mathbb{Z}_3^N$ that contains no multicolored sunflower. In particular, if Conjecture 6 is true for ϵ_0, then the strong USP capacity is at most $(3/2^{2/3})^{1-\epsilon_0}$.*

Proof Let $\mathcal{F} \subseteq \mathbb{Z}_3^{3n}$ be a local strong USP for which every $v \in \mathcal{F}$ has equal numbers of 0's, 1's and 2's. Our goal will be to produce a collection $\mathcal{F}' \subseteq S_0 \times S_1 \times S_2 \subseteq (\mathbb{Z}_3^n)^3$ such that (1) $\mathcal{F}'$ is a collection of *pairwise disjoint* ordered sunflowers, and (2) every ordered sunflower in $S_0 \times S_1 \times S_2$ is in $\mathcal{F}'$. Such a collection then contains no multicolored sunflowers.

For $x \in \mathbb{Z}_3^{3n}$ and $I \subseteq [n]$, we denote by x_I the projection of x to the coordinates I. Fix a vector $v \in \mathcal{F}$ and let $I = \{i : v_i = 0\}$, $J = \{j : v_j = 1\}$ and $K = \{k : v_k = 2\}$. We define

$$\begin{aligned} T_0^{(v)} &= \{x : x_I = 0^n, x_J \in \{1,2\}^n, x_K \in \{1,2\}^n\} \\ T_1^{(v)} &= \{y : y_I \in \{1,2\}^n, y_J = 0^n, y_K \in \{1,2\}^n\} \\ T_2^{(v)} &= \{z : z_I \in \{1,2\}^n, z_J \in \{1,2\}^n, z_K = 0^n\}. \end{aligned}$$

We identify $\{1,2\}^n$ with the integers $\{0,1,2,\ldots,2^n-1\}$ arbitrarily and denote this lift of $w \in \{1,2\}^n$ to the integers by $\overline{w}$.

Define functions $a^{(v)} : T_0^{(v)} \to \mathbb{Z}$, $b^{(v)} : T_1^{(v)} \to \mathbb{Z}$, and $c^{(v)} : T_2^{(v)} \to \mathbb{Z}$ as follows, where s is the integer $\lceil 3 \cdot 2^n/2 \rceil + 1$:

$$\begin{aligned} a^{(v)}(x) &= ((\overline{x_J}) - s)^2 + 2((\overline{x_J}) - s)(\overline{-x_K}) \\ b^{(v)}(y) &= (\overline{y_K})^2 + 2(\overline{y_K})(\overline{-y_I}) \\ c^{(v)}(z) &= (\overline{z_I})^2 + 2(\overline{z_I})((\overline{-z_J}) - s). \end{aligned}$$

These functions and the following lemma are used in [BCS97] (in a presentation of material originally appearing in [Str87]), to show, in their language, that the matrix multiplication tensor has a large diagonal which is a *combinatorial degeneration*. We use it for a slightly different purpose here.

Lemma 3.8 ([BCS97] Lemma 15.31) *If $(x,y,z) \in T_0^{(v)} \times T_1^{(v)} \times T_2^{(v)}$ form a sunflower, $a^{(v)}(x) + b^{(v)}(y) + c^{(v)}(z) \geq 0$. Moreover, the set*

$$\Delta^{(v)} = \{(x,y,z) \in T_0^{(v)} \times T_1^{(v)} \times T_2^{(v)} \mid \{x,y,z\} \text{ form a sunflower} \\ \text{and } a^{(v)}(x) + b^{(v)}(y) + c^{(v)}(z) = 0\}$$

is a collection of pairwise disjoint ordered sunflowers with cardinality at least $\lceil 3 \cdot 2^{2n}/4 \rceil$.

We sketch the proof here for completeness.

Proof When (x,y,z) form an ordered sunflower, we have $y_I = -z_I$, $x_J = -z_J$ and $x_K = -y_K$, and then setting $i = \overline{z_I}$, $j = \overline{x_J}$, and $k = \overline{y_K}$, we have

$$a^{(v)}(x) + b^{(v)}(y) + c^{(v)}(z) = (j-s)^2 + 2(j-s)k + k^2 + 2ki + i^2 + 2i(j-s) = (i+j+k-s)^2.$$

Clearly this function is non-negative, and equals 0 exactly when $i + j + k = s$. Since each of x, y, and z determines two of i, j, k and any two of i, j, k determine the third under this constraint (and thus determine the entire triple), the sunflowers in $\Delta^{(v)}$ are pairwise disjoint. The cardinality of $\Delta^{(v)}$ is an easy calculation. □

Now, define $T_0 = \bigcup_{v\in\mathcal{F}} T_0^{(v)}$, $T_1 = \bigcup_{v\in\mathcal{F}} T_1^{(v)}$, and $T_2 = \bigcup_{v\in\mathcal{F}} T_2^{(v)}$. We note that any ordered sunflower $(x,y,z) \in T_0 \times T_1 \times T_2$ must have $(x,y,z) \in T_0^{(v)} \times T_1^{(v)} \times T_2^{(v)}$ for some $v \in \mathcal{F}$, because otherwise by the strong USP property, there is some coordinate i in which exactly two of $\{x_i, y_i, z_i\}$ equal 0, and so $\{x,y,z\}$ cannot be a sunflower. We will use this observation, together with Lemma 3.8 to produce our final construction.

Notice that the $a^{(v)}, b^{(v)}, c^{(v)}$ define in a consistent way functions a, b, c from T_0, T_1, T_2, respectively, to $\mathbb{Z}$, because the $T_0^{(v)}$ are disjoint sets (and the same for the $T_1^{(v)}$ and the $T_2^{(v)}$). Now, consider the ℓ-fold direct product of the three sets, T_0^ℓ, T_1^ℓ, T_2^ℓ, and the functions $A : T_0^\ell \to \mathbb{Z}$, $B : T_1^\ell \to \mathbb{Z}$, and $C : T_2^\ell \to \mathbb{Z}$ defined by $A(X) = \sum_i a(X_i)$, $B(Y) = \sum_i b(Y_i)$, and $A(Z) = \sum_i c(Z_i)$. We claim that

$$\Delta = \{(X,Y,Z) \in T_0^\ell \times T_1^\ell \times T_2^\ell : \{X,Y,Z\} \text{ form a sunflower and } A(X) + B(Y) + C(Z) = 0\}$$

is a collection of pairwise disjoint ordered sunflowers with cardinality at least

$$(|\mathcal{F}| \cdot \lceil 3 \cdot 2^{2n}/4 \rceil)^\ell.$$

This is because each (X_i, Y_i, Z_i) must lie in $T_0^{(v_i)} \times T_1^{(v_i)} \times T_2^{(v_i)}$ for some $v_i \in \mathcal{F}$ (as we observed above), and then by the first part of Lemma 3.8,

$$A(X) + B(Y) + C(Y) = 0 \Leftrightarrow a(X_i) + b(Y_i) + c(Z_i) = 0 \text{ for all } i.$$

Thus $\Delta = \left(\bigcup_{v\in\mathcal{F}} \Delta^{(v)}\right)^\ell$.

We are not done, however, because $T_0^\ell \times T_1^\ell \times T_2^\ell$ may contain an ordered sunflower (X,Y,Z) not already in Δ, and this happens exactly when $A(X)+B(Y)+C(Z) > 0$. One final trick will fix this problem, and we describe it next. If a, b, c take values in $[-M, M]$, then A, B, C take values in $[-\ell M, \ell M]$. Thus there exist α, β, γ such that at least a $1/(2\ell M)^3$ fraction of the triples (X,Y,Z) in Δ satisfy $A(X) = \alpha, B(Y) = \beta, C(Z) = \gamma$. So, define $S_0 = \{X \in T_0^\ell : A(X) = \alpha\}$, $S_1 = \{Y \in T_1^\ell : B(Y) = \beta\}$, $S_2 = \{Z \in T_2^\ell : C(Z) = \gamma\}$, and

$$\mathcal{F}' = \Delta \cap (S_0 \times S_1 \times S_2).$$

Then $\mathcal{F}'$ is a collection of pairwise disjoint ordered sunflowers (because Δ is) for which every ordered sunflower $(X,Y,Z) \in S_0 \times S_1 \times S_2$ is in $\mathcal{F}'$, as desired. The cardinality of $\mathcal{F}'$ is at least

$$\frac{(|\mathcal{F}| \cdot \lceil 3 \cdot 2^{2n}/4 \rceil)^\ell}{(2\ell M)^3}.$$

If the strong USP capacity is at least c, then by Lemma 3.6, for infinitely many n, there exist balanced, local strong USPs $\mathcal{F} \subseteq \mathbb{Z}_3^{3n}$ with cardinality at least $(c - o(1))^{3n}$. Taking ℓ sufficiently large in the above expression, the theorem follows. □

Cohn et al. proved that the strong USP capacity is at least $2^{2/3}$ (Proposition 3.8 in [CKSU05]). Applying Theorem 3.7, we obtain a lower bound of $(2^{4/3} - o(1))^n > 2.51^n$ on the maximum cardinality of a collection of ordered sunflowers in $\mathbb{Z}_3^n \times \mathbb{Z}_3^n \times \mathbb{Z}_3^n$ containing no multicolored sunflower. Notice that this is larger than the best known lower bound on the maximum cardinality of 3-sunflower-free subsets of $\mathbb{Z}_3^n$ [Edel04].

Finally, we show that if Conjecture 4 is in fact false, then Conjecture 7 is true, and hence the exponent of matrix multiplication is 2. The complete picture with the two matrix-multiplication related conjectures included is in Figure 2. Notice the interesting conclusion that the "no three disjoint equivoluminous subsets" conjecture of [CW90] actually implies the (seemingly very different) strong USP conjecture of [CKSU05].

$$\begin{tikzcd}
 & \text{Conj. 7 false} \arrow[dr, Rightarrow, "Thm.3.9"] & \text{Conj. 3} \arrow[r, Leftrightarrow, "Thm.\ 2.6"] \arrow[d, Rightarrow] & \text{Conj. 1} \arrow[d, Rightarrow, "Thm.\ 2.3"] & \\
\text{Conj. 6} \arrow[ur, Rightarrow, "Thm.3.7"] \arrow[r, Rightarrow] & \text{Conj. 5} \arrow[r, Rightarrow] & \text{Conj. 4} \arrow[r, Leftrightarrow, "Thm.\ 2.7"] & \text{Conj. 2} \arrow[r, Rightarrow, "Thm.3.2"] & \text{Conj.[CW90] false}
\end{tikzcd}$$

Figure 2: Sunflower conjectures and matrix multiplication conjectures. Everything in this paper is labeled a "conjecture" for uniformity of presentation; however some seem more likely to be true than others. In particular, it would not be overly surprising if everything to the left of Conjecture 3 and 4 in this figure turned out to be false.

Theorem 3.9 *If the strong USP capacity is at most $(3/2^{2/3})^{1-\epsilon_0}$ for some $\epsilon_0 > 0$ then Conjecture 4 holds with $\epsilon = \epsilon_0/2$ and n large enough.*

Proof Assume for convenience that $D = \frac{1}{3} \cdot \binom{n}{n/3}$, for some integer n divisible by 3 (we later show that this can be assumed w.l.o.g.) and that we are given a 3-sunflower-free collection $\mathcal{F} \subseteq \mathbb{Z}_D^m$ of size $|\mathcal{F}| \geq D^{(1-\epsilon)m}$, for m sufficiently large. We will rely on the following (special case of a) theorem of Baranyai [Bar75].

Theorem 3.10 *There is a set G of D vectors in $\mathbb{Z}_3^n$, each having exactly $n/3$ zeros, $n/3$ ones and $n/3$ twos, where every subset of size $n/3$ of $[n]$ appears exactly once as the set of all occurrences of a* 0,1 *or* 2 *in some vector*

We shall create a family, corresponding to $\mathcal{F}$, in Z_3^{nm}. Identify the set $[D]$ with the elements of G (arbitrarily). Given a vector in $\mathcal{F}$ we replace each symbol by the corresponding member of G and concatenate all those sets to obtain a vector of length nm. This gives a new family $\mathcal{F}'$ of $D^{(1-\epsilon)m}$ vectors in $\mathbb{Z}_3^{nm}$. As

$$|\mathcal{F}'| \geq D^{(1-\epsilon)m} = \left(\frac{1}{3} \cdot \binom{n}{n/3}\right)^{(1-\epsilon)m} = 2^{H(1/3)(1-\epsilon)nm+o(nm)} = \binom{nm}{nm/3}^{1-\epsilon+o(1)} > \binom{nm}{nm/3}^{1-\epsilon_0}$$

we get, by the assumption that the strong USP capacity is at most $(3/2^{2/3})^{1-\epsilon_0}$, that there are three vectors u', v', w' (not all equal) in $\mathcal{F}'$ such that the sets $\{i : u'_i = 0\}$, $\{j : v'_j = 1\}$ and $\{l : w'_l = 2\}$ form a 3-sunflower. It is not hard to verify that the 'original' vectors v, u and w of $\mathcal{F}$ form a 3-sunflower. Indeed, suppose that in some coordinate i we have that the set $\{u_i, v_i, w_i\}$ contains exactly two distinct values, say $u_i = \alpha$, $v_i = \alpha$ and $w_i = \beta$. Let A_α and

A_β be the corresponding members of G. By the construction of G, the sets $\{j \mid (A_\alpha)_j = 3\}$ and $\{j \mid (A_\beta)_j = 3\}$ are different. Hence, $\{j \mid (A_\beta)_j = 3\}$ intersects at least one of the sets $\{j \mid (A_\alpha)_j = 1\}$ or $\{j \mid (A_\alpha)_j = 2\}$. However, since $\{j \mid (A_\alpha)_j = 1\}$ and $\{j \mid (A_\alpha)_j = 2\}$ are disjoint, this contradicts the assumption that u', v', w' form a 3-sunflower.

To complete the proof we argue that we can assume w.l.o.g. that $D = \frac{1}{3} \cdot \binom{n}{n/3}$, for some integer n divisible by 3. Indeed, we can always find an integer n divisible by 3, such that $\frac{1}{3} \cdot \binom{n-3}{(n-3)/3} < D \leq \frac{1}{3} \cdot \binom{n}{n/3}$. As $\binom{n-3}{(n-3)/3} > \frac{4}{27} \cdot \binom{n}{n/3}$ it follows that $D^{(1-\epsilon)m} > \left(\frac{4}{27} \cdot \binom{n}{n/3}\right)^{(1-\epsilon)m} > \binom{n}{n/3}^{(1-1.1\epsilon)m}$, for large enough n. Set $D' = \binom{n}{n/3}$ and view $\mathcal{F}$ as a subset of $\mathbb{Z}_{D'}^m$ of size at least $D'^{(1-1.1\epsilon)m}$. As we picked $\epsilon < \epsilon_0/2$ the calculations above are not affected by this change. $\square$

Acknowledgment We thank Adam Marcus for helpful discussions in an early stage of this research. We thank Henry Cohn, Bobby Kleinberg, and Balázs Szegedy for help in formulating the weak sunflower conjecture in $\mathbb{Z}_D^n$, and for useful discussions.

References

[AB87] N. Alon and R. B. Boppana. The monotone circuit complexity of Boolean functions. Combinatorica 7 (1987), 1–22.

[AP01] N. Alon and P. Pudlak. Constructive lower bounds for off-diagonal Ramsey numbers. Israel J. Math. 122 (2001), 243–251.

[Bar75] Zs. Baranyai. On the factorization of the complete uniform hypergraph. In *Infinite and finite sets, Proc. Coll. Keszthely, 1973, (A. Hajnal, R. Rado and V.T. Sós, eds.), Colloquia Math. Soc. János Bolyai 10.* North-Holland, 1975.

[BK11] M. Batemand and N. H. Katz. *New Bounds on cap sets.* In *arXiv:1101.5851v1*, 2011.

[BCS97] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic Complexity Theory.* Springer, 1997.

[CKSU05] H. Cohn, R. D. Kleinberg, B. Szegedy, and C. Umans. Group-theoretic algorithms for matrix multiplication. In *Proceedings of the 46th Annual FOCS*, pages 379–388, 2005.

[CU03] H. Cohn and C. Umans. A group-theoretic approach to fast matrix multiplication. In *Proceedings of the 44th Annual FOCS*, pages 438–449, 2003.

[CW90] D. Coppersmith and S. Winograd. Matrix multiplication via arithmetic progression. *J. of Symbolic Computation*, 9:251–280, 1990.

[DEGKM97] W. A. Deuber, P. Erdős, D. S. Gunderson, A. V. Kostochka, and A. G. Meyer. Intersection statements for systems of sets. J. Combin. Theory Ser. A 79 (1997), no. 1, 118–132.

[Edel04] Y. Edel. Extensions of generalized product caps. *Designs, Codes and Cryptography* 31 (2004), no. 1, 5–14.

[ER60] P. Erdős and R. Rado. Intersection theorems for systems of sets. *J. London Math. Soc.*, 35:85–90, 1960.

[ER69] P. Erdős and R. Rado. Intersection theorems for systems of sets II. *J. London Math. Soc.*, 44:467–479, 1969.

[Erd71] P. Erdős. Some unsolved problems in graph theory and combinatorial analysis. In *Combinatorial Mathematics and its Applications (Proc. Conf., Oxford, 1969)*, pages 97–109. Academic Press, London, 1971.

[Erd75] P. Erdős. Problems and results on finite and infinite combinatorial analysis. In János Bolyai, editor, *Infinite and finite sets (Colloq., Keszthely, 1973; dedicated to P. Erdős on his 60th birthday) Vol. I; Colloq. Math. Soc.*, volume 10, pages 403–424. North-Holland, Amsterdam, 1975.

[Erd81] P. Erdős. On the combinatorial problems which I would most like to see solved. *Combinatorica*, 1(1):25–42, 1981.

[ES78] P. Erdős and E. Szemerédi. Combinatorial properties of systems of sets. *J. Combinatorial Theory Ser. A*, 24(3):308–313, 1978.

[Fu91] Z. Füredi. Turán type problems. In *Surveys in combinatorics*, 1991 (Guildford, 1991), 253-300, London Math. Soc. Lecture Note Ser., 166, Cambridge Univ. Press, Cambridge, 1991.

[Gat88] J. von zur Gathen. Algebraic complexity theory. *Annual review of computer science*, 3:317–347, 1988.

[Ju01] Stasys Jukna. *Extremal Combinatorics.* Springer, 2001.

[Ko97] A. V. Kostochka. A bound of the cardinality of families not containing Δ-systems. In: *The mathematics of Paul Erdős, II*, 229-235, Algorithms Combin., 14, Springer, Berlin, 1997.

[Me95] R. Meshulam. On subsets of finite abelian groups with no 3-term arithmetic progressions. J. Combin. Theory Ser. A 71 (1995), 168–172.

[Ra85] A. A. Razborov. Lower bounds on the monotone complexity of some Boolean functions, (Russian). Dokl. Akad. Nauk SSSR 281 (1985), no. 4, 798–801.

[SS42] R. Salem and D. Spencer. On sets of integers which contain no three in arithmetic progression. *Proc. Nat. Acad. Sci. (USA)*, 28:561 563, 1942.

[Spe77] J. Spencer. Intersection theorems for systems of sets. *Canadian Math Bulletin*, 20(2):249–254, 1977.

[Str69] V. Strassen. Gaussian elimination is not optimal. *Numer. Math*, 13:354–356, 1969.

[Str87] V. Strassen. Relative bilinear complexity and matrix multiplication. *J. Reine Angew. Math.*, 375/376:406–443, 1987.