Towards dimension expanders over finite fields

Zeev Dvir, Amir Shpilka

Presented by Zuzana Safernová

Let $\mathbb{F}$ be a field.

Definition 1 *Let $A_1, \ldots, A_k : \mathbb{F}^n \to \mathbb{F}^n$ be linear mappings. The set $\mathcal{A} = \{A_i\}_{i=1}^k$ is a (d, α)-*dimension expander *if for every subspace $V \leq \mathbb{F}^n$, $\dim V \leq d$ we have*

$$\dim\left(V + \sum_{i=1}^{k} A_i(V)\right) \geq (1+\alpha) \cdot \dim V.$$

$\mathcal{A}$ is *explicit* if there exists a poly(n)-time algorithm that, on input n, outputs $\mathcal{A}$.

Problem 2 *Construct an explicit (d, α)-dimension expander $\mathcal{A} = \{A_i\}_{i=1}^k$, with $d = \Omega(n)$, $\alpha = \Omega(1)$ and $k = O(1)$.*

Theorem 3 *There exists a constant $\alpha > 0$ such that for every n there exists a set $\mathcal{A}(n)$ of $O(\log n)$ linear mappings from $\mathbb{F}^n$ to $\mathbb{F}^n$ that is an $\big(\Omega(n), \alpha\big)$-dimension expander. Moreover, the construction is explicit and independent of the field $\mathbb{F}$.*

Theorem 4 *There exists a constant $k_0 > 0$ such that for every n there exists a set $\mathcal{A}(n)$ of k_0 linear mappings from $\mathbb{F}^n$ to $\mathbb{F}^n$ that is an $\big(\Omega(n), \Omega(1/\log n)\big)$-dimension expander. Moreover, the construction is explicit and independent of the field $\mathbb{F}$.*

Towards the proofs

Let $v = (v_1, \ldots, v_n) \in \mathbb{F}^n$ be a non-zero vector.

- $\deg(v) :=$ the largest index $i \in [n]$ such that $v_i \neq 0$
- $D_V := \{\deg(v) | v \in V, v \neq 0\}$, where $V \leq \mathbb{F}^n$ and $\dim V = k$; note that $|D_V| = k$
- **Claim.** Let $D_{A(V)} = \{\deg(A(v)) | v \in V, A(v) \neq 0\}$, where A is a linear mapping from $\mathbb{F}^n$ to $\mathbb{F}^n$, then $\dim(V + A(V)) \geq |D_V \cup D_{A(V)}|$.
- Let H be a finite group, $M \in H$ the set of generators. The *Cayley graph Cay(H,M)* induced by M on H is the graph with vertex set H and $u \sim v$ iff $u \cdot v^{-1} \in M \cup M^{-1}$.

Theorem 5 (Wigderson, Xiao) *There exist constants $\beta, \gamma > 0$ and an algorithm T such that on input n, the algorithm runs in poly(n) time and returns a set $J \subset [n]$ of size $O(\log n)$ such that J generates $(\mathbb{Z}_n, +)$ and the graph* $\mathrm{Cay}(\mathbb{Z}_n, J)$ *is a $(\gamma n, \beta)$-expander.*

- $s_1, \ldots, s_n : \mathbb{F}^n \to \mathbb{F}^n$ are the n right cyclic shifts of coordinates of $\mathbb{F}^n$, i.e. $s_j(v) = (v_{n-j+1}, \ldots, v_n, v_1, v_2, \ldots, v_{n-j})$.
- $P_L, P_R : \mathbb{F}^n \to \mathbb{F}^n$ are defined as $P_L(v', v'') = (v'', \bar{0})$, $P_R(v', v'') = (\bar{0}, v')$, where v' (v'') denotes the first (last) $n/2$ (n even) coordinates of v.

Lemma 6 *Let $n = p + 1$ for an odd prime p. Let S_{p+1} denote the set of permutations on $\{1, \dots, p+1\}$. Let $s_1, \dots, s_p \in S_{p+1}$ denote the p right cyclic shifts on the set $\{1, \dots, p\}$ such that $s_j(p+1) = p+1$ for every j. Then, there exists a set $M \in S_{p+1}$ of size $|M| \leq 7$ such that for every $j \in [p]$, the permutation s_j can be written as a word of length $O(\log p)$ using elements from $M \cup M^{-1}$. Moreover, this set can be generated in time polynomial in n.*

- $P \colon \mathbb{F}^n \to \mathbb{F}^n$ is defined as $P(v) = (v_{(p+3)/2}, \dots, v_{p+1}, 0, \dots, 0)$.
- $Q_p \colon \mathbb{F}^n \to \mathbb{F}^n$ is defined as $Q_p(v) = (v_{p+2}, \dots, v_n, 0, \dots, 0)$.

Constructions

- Theorem 3: $\mathcal{A}(n) = \{s_j\}_{j \in J} \cup \{P_L, P_R\}$ is $(\gamma' n, \beta')$-dimension expander, where $n = 2m$, $\gamma', \beta' > 0$, J given by Theorem 5, so $|J| \leq O(\log m)$.
- Theorem 4 and $n = p + 1$, p prime: $\mathcal{A}(n) = M \cup M^{-1} \cup \{P\}$ is an $\big(n/5, \Omega(1/\log n)\big)$-dimension expander, where M is given by Lemma 6, and $|M| \leq 7$.
- Theorem 4: $\mathcal{A}'(n) = \mathcal{A}(p+1) \cup \{Q_p\}$ is an $\big(n/10, \Omega(1/\log n)\big)$-dimension expander, where $\mathcal{A}(p+1)$ is dimension expander given above (we treat the mappings from $\mathcal{A}(p+1)$ as acting on $\mathbb{F}^n$ by applying them only on the first $p+1$ coordinates and leaving the remaining coordinates untouched).