Density increment for 4-AP's

$f: \mathbb{Z}_N \to [-1,1]$, $\quad \phi(x) = e\left(\frac{ax^2+bx}{N}\right)$, $\eta > 0$

$\langle f, \phi \rangle = \left| \mathbb{E}_{x\in\mathbb{Z}_N} f(x)\, e\left(-\frac{ax^2+bx}{N}\right) \right| \geq \eta$ "quadratic bias"

Lemma 1 $\quad f: \mathbb{Z}_N \mapsto [-1,1]$, $\lambda \in \mathbb{Z}_N$ s.t.

$$\mathbb{E}_{k\in\mathbb{Z}_N} |\widehat{\Delta_k f}(2\lambda k)|^2 \geq \eta > 0$$

$(\Delta_k f(x) = f(x)\bar{f}(x+k))$

Then $\exists r \in \mathbb{Z}_N$: $\left| \mathbb{E}_{n\in\mathbb{Z}_N} f(n)\, e\left(\frac{\lambda n^2 + rn}{N}\right) \right| \geq \eta^{\frac{1}{2}}$.

Proof

$$\mathbb{E}_{k\in\mathbb{Z}_N} \left| \mathbb{E}_x f(x) f(x+k)\, e\left(-\frac{2x\lambda k}{N}\right) \right|^2 \quad ; \quad y = x+h$$

$$= \mathbb{E}_{k\in\mathbb{Z}_N} \mathbb{E}_{x,h} f(x) f(x+k) f(x+h) f(x+k+h)\, e\left(\frac{2\lambda k h}{N}\right)$$

$$2kh = (x+k+h)^2 + x^2 - (x+k)^2 - (x+h)^2$$

$$g(x) = f(x)\, e(\lambda x^2/N)$$

$$= \mathbb{E}_{x,h,k}\, g(x)\, \bar{g}(x+k)\, \bar{g}(x+h)\, g(x+h+k) = \|g\|_{U^2}^4 = \sum_r |\hat{g}(r)|^4$$

$$\leq \left(\max_r |\hat{g}(r)|^2\right) \cdot 1$$

$\exists r$: $\quad |\hat{g}(r)| = \left| \mathbb{E}_x f(x)\, e\left(\frac{\lambda x^2 - rx}{N}\right) \right| \geq \eta^{1/2}$

$\square$

There is a progression $P \subseteq \mathbb{Z}_N$, s.t. for $\gg \alpha^C |P|$ values of $k \in P$; $|\widehat{\Delta_k f_A}(\underbrace{\mu + 2\lambda k}_{\phi(k)})| \gg \alpha^C$.

$$\Rightarrow \quad \mathbb{E}_{k \in P} |\widehat{\Delta_k f}(\mu + 2\lambda k)|^2 \gg \alpha^C$$

where $|P| \gg \exp(-\alpha^{-C})\, N$.

<u>Lemma 2.</u> $\forall x \in \mathbb{Z}_N \ \exists r_x \in \mathbb{Z}_N$ s.t.

$$\mathbb{E}_{x \in \mathbb{Z}_N} \left| \mathbb{E}_{\ell \in P + x} f(\ell)\, e\left(-\frac{\lambda \ell^2 + r_x \cdot \ell}{N}\right)\right| \gg \alpha^C$$

<u>Proof</u>

$$H = \mathbb{E}_{k \in P} \mathbb{E}_{x,h} f(x) f(x+k) f(x+h) f(x+k+h)\, e\left(\frac{(\mu + 2\lambda k)h}{N}\right)$$

Writh $h = y + \ell$; $y \in \mathbb{Z}_N$, $\ell \in P$; note that

$$\mathbb{E}_h g(h) = \mathbb{E}_{y \in \mathbb{Z}_N} \mathbb{E}_{\ell \in P}\, g(y + \ell)$$

$$H = \mathbb{E}_{x,y \in \mathbb{Z}_N} \mathbb{E}_{k,h \in P} f(x) \ldots f(x+k+h)\, e\left(\frac{(2\lambda k + \mu)(y+\ell)}{N}\right)$$

$$(2\lambda k + \mu)(y + \ell) = 2\lambda \cdot k\ell + 2\lambda k y + \mu \ell + \cancel{\mu y}$$

and $\quad 2k\ell = (k+\ell)^2 - k^2 - \ell^2$

$$LH \le \mathbb{E}_{x,y \in \mathbb{Z}_N} \left| \mathbb{E}_{k,\ell \in P}\, g_1(k)\, g_2(\ell)\, g_3(k+\ell)\right|$$

where
$$g_1(k) = g_{1,x,y}(k) = f(x+k)\, e\left(\frac{2\lambda k y - \lambda k^2}{N}\right) \cdot 1_P(k)$$
$$g_2(\ell) = g_{2,x,y}(\ell) = f(x+\ell)\, e\left(\frac{\mu\ell - \lambda \ell^2}{N}\right) \cdot 1_P(\ell)$$
$$g_3(k+\ell) = g_{3,x,y}(k+\ell) = f(x+k+\ell)\, e\left(\lambda(k+\ell)^2/N\right) 1_{P+P}(k+\ell)$$

$$\left|\mathbb{E}_{k,l\in\mathbb{Z}_N}\, g_1(k)\, g_2(l)\, \underbrace{g_3(k+l)}_{\sum_r \hat{g}_3(r)\, e\left(\frac{r(k+l)}{N}\right)}\right| \le \sum_r |\hat{g}_1(-r)\,\hat{g}_2(-r)\,\hat{g}_3(r)|$$

$$\le \left(\max_r |\hat{g}_2(r)|\right)\underbrace{\left(\sum_r |\hat{g}_1(r)|^2\right)^{1/2}}_{\left(\mathbb{E}_{x\in\mathbb{Z}_N}|g_1(x)|^2\right)^{1/2}}\underbrace{\left(\sum_r |\hat{g}_3(r)|^2\right)^{1/2}}_{\left(\mathbb{E}_x |g_3(x)|^2\right)^{1/2}}$$

$$\le \left(\max_r |\hat{g}_2(r)|\right)\left(\frac{|P|}{N}\right)^{1/2}\left(\frac{|P|}{N}\right)^{1/2} = \left(\max_r |\hat{g}_2(r)|\right)\frac{|P|}{N}$$

$$\underline{LH} \le \mathbb{E}_{x,y\in\mathbb{Z}_N}\left(\frac{N}{|P|}\right)^2 \frac{|P|}{N}\left(\max_r |\hat{g}_{2,x,y}(r)|\right)$$

$$\mathbb{E}_{x,y\in\mathbb{Z}_N}\left(\max_r |\hat{g}_{2,x,y}(r)|\right) \gg \cancel{\frac{|P|}{N}}\,\alpha^c$$

where $\max_r |\hat{g}_{2,x,y}(r)| = \frac{1}{N}\left|\sum_{l\in\mathbb{Z}_N} f(x+l)\, e\left(\frac{\mu l - \lambda l^2 - r_x l}{N}\right) 1_P(l)\right|$

$$= \cancel{\frac{|P|}{N}}\left|\mathbb{E}_{l\in P} f(x+l)\, e\left(\frac{-\lambda l^2 + r_x' l}{N}\right)\right|$$

$$\mathbb{E}_{x\in\mathbb{Z}_N}\left|\mathbb{E}_{l\in P+x}\, e\left(\frac{-\lambda l^2 + r_x'' l}{N}\right)\right| \gg \alpha^c$$

$\square$

Weyl's ineq. & density increment

Lemma 1. Let $P = \{a + jd \,;\, 1 \le j \le R\} \subseteq \mathbb{Z}_N$ be a progr., and let $\psi(x) = rx$; $r \in \mathbb{Z}_N$.

Then P can be partitioned into progr. $P_1, P_2, \dots, P_M$ s.t. $|P_i| \approx R^{1/4}$ and $\forall i \le M$ $\forall$ $x, y \in P_i$

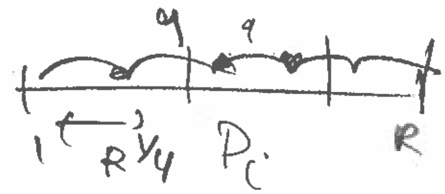
$$\left|e\left(\frac{\psi(x)}{N}\right) - e\left(\frac{\psi(y)}{N}\right)\right| \ll R^{-1/4}.$$

Proof Let $1 \le q \le R^{\frac{1}{2}}$ s.t. $\| q \, r/N \| \le R^{-\frac{1}{2}}$.

- WLOG can assume $P = [1, R]$, b/c

$$e\left(\psi\left(\frac{a+xd}{N}\right)\right) = \cancel{e\left(\frac{ra}{N}\right)} \underbrace{e\left(\frac{x\, rd}{N}\right)}, \quad \tilde{r} = rd$$

- Partition $P = [1, R]$ into progressions (mod q), and each progr. into "intervals" of length (size) $\approx R^{1/4}$, this gives



$$P = \bigcup_{i=1}^{M} P_i\,; \quad M \approx R^{3/4}.$$

- Fix $i \le M$, $x, y \in P_i$

$$\left| e\left(\frac{rx}{N}\right) - e\left(\frac{ry}{N}\right) \right| \le \left| e\left(\frac{r(y-x)}{N}\right) - 1 \right| \ll \left\| \frac{r(y-x)}{N} \right\|$$

$$x = \cancel{b} + uq, \quad y = \cancel{b} + vq; \quad 1 \le u, v \le R^{1/4}$$

$$\left\| \frac{rq(u-v)}{N} \right\| \le \left\| \frac{rq}{N} \right\| |u-v| \le R^{-1/2} R^{1/4} \le R^{-1/4}$$

$\square$

Thm (Heibron prop.) Let $\alpha \in \mathbb{R}$, $M \in \mathbb{N}$.

Then $\exists\, 1 \le m \le M$ s.t. $\| m^2 \alpha \| \le (\log M)\, M^{-1/3}$

Conjecture $\exists\, m \le M$ s.t. $\| m^2 \alpha \| \le C_\varepsilon M^{-1+\varepsilon}$ $(\forall \varepsilon > 0)$

Lemma 2. Let $P = \{a + jd;\ 1 \le j \le R\}$, $\psi(x) = rx^2 + sx$.

Then P can be partitioned into progr., $P_1, P_2, \dots, P_M$ each of length $\approx R^{\frac{1}{128}}$ s.t. $\forall i \le M$, $\forall x, y \in P_i$

$$|e(\psi(x)/N) - e(\psi(y)/N)| \ll R^{-\frac{1}{128}}.$$

Pf: $\psi(a + xd) = \tilde{\psi}(x) + b \Rightarrow$ WLOG: $P = [1, R]$.

Heilbronn $\Rightarrow \exists\ 1 \le q \le R^{1/2}$ st $\|q^2 r/N\| \le R^{-\frac{1}{8}}$

Partition $[1, R]$ int progr. mod q, then each into intervals = sup. prog. of size $\approx R^{\frac{1}{32}}$.

Let $b + xq, b + yq \in P_i$; $1 \le x, y \le R^{1/4}$

$$|e(\tfrac{r(b+xq)^2}{N}) - e(\tfrac{r(b+yq)^2}{N})| \ll \underbrace{\left\| \frac{(x^2 - y^2) r^2 q}{N} \right\|}_{\ll R^{\frac{1}{16}} R^{-\frac{1}{8}}} + \underbrace{\left\| \frac{(x-y)\, 2rbq}{N} \right\|}_{\text{Lemma 1.}}$$

Lemma 1′ $P \subseteq \mathbb{Z}/N$ progr of size N, then P can be partitioned into $\mathbb{Z}$-progressions $P_1, \dots, P_M$; $|P_i| \approx R^{1/2}$ $\forall\, 1 \le i \le M$.