הוכחת למה 2.2 ב [IKW09] – גרסה מתוקנת

<u>למה 2.2</u>

יהא $U = F_q^m$.

יהיו V_0 ו- V_1 זוג תתי-מרחבים וקטוריים לינאריים אורתוגונליים מעל U.

יהא $X \subseteq V_0 + V_1$ תת קבוצה בגודל יחסי μ, קרי $\frac{|X|}{|V_0+V_1|} = \mu$.

ויהא $W \subset V_1$ תת מרחב לינארי אקראי של V_1 בגודל $|W| = q^r$.

אזי מתקיים (**צ"ל**): $\Pr\left[\left|\frac{|(V_0+W)\cap X|}{|V_0+W|} - \mu\right| \geq \frac{\mu}{2}\right] \leq \frac{(4+o(1))q^2}{|W|\mu}$.

<u>הוכחה</u>

נתחיל עם $X \subseteq V_0 + V_1 \setminus V_0$:

עבור W הנתון - תת מרחב לינארי מסדר r - יהא $w_1,\dots,w_t \in F_q^r$ אוסף וקטורים קבוע בת"ל בזוגות, כש- $t = \frac{q^r-1}{q-1}$. אוסף כזה מובטח לנו מלמה 2.1 עבור תתי מרחבים לינארים של F_q^r ממימד 1, זרים פרט ל- 0.

ע"פ טענה 2.4 ב [IJKW08], t הוקטורים המתאימים ל $w_1,\dots,w_t$ ב- W הם בת"ל בזוגות ומתפלגים אחיד מעל U. מה שעושים בפועל בטענה 2.4 הוא להגריל בסיס רנדומלי ל W, ואז הוקטורים המתאימים הם אקראיים ובת"ל בזוגות. נסמן את הוקטורים המתאימים $\omega_1,\dots,\omega_t$.

עתה, נפלח את $V_0 + W$ לפרוסות – נגדיר $B_i \triangleq \bigcup_{j=1}^{t}(V_0 + i\omega_j), i \in F_q \setminus \{0\}$, ומתקיים ש $B = \bigcup_{i \in F_q \setminus \{0\}} B_i = V_0 + W \setminus V_0$.

נתחיל לטפל ב X ונגדיר פונקציית אינדיקטור $I : (V_0 + V_1 \setminus V_0) \to \{0,1\}$: $I(u) = \begin{cases} 1 & u \in X \\ 0 & else \end{cases}$

מתקיים: $\mathrm{Exp}[I] = \mu = (1 \pm o(1))\mu$

עבור i קבוע מתקיים מ Chebyshev Bound של למה 2.2 כי:

$$\Pr\left[\left|\sum_{x\in B_i} I(x)-|B_i|\mu\right|\geq\frac{|B_i|\mu}{2}\right]\leq\frac{4}{|B_i|\mu}=\frac{4}{\mu t}$$

$$\Rightarrow\Pr\left[\left|\sum_{x\in B_i} I(x)-|B_i|\left(1\pm o(1)\right)\mu\right|\geq\frac{|B_i|\left(1\pm o(1)\right)\mu}{2}\right]\leq\frac{4+o(1)}{|B_i|\mu}=\frac{4+o(1)}{\mu t}$$

$$\Rightarrow\Pr\left[\left|\frac{1}{|B_i|}\sum_{x\in B_i} I(x)-\mu\right|\geq\frac{\mu}{2}\right]\leq\frac{4+o(1)}{\mu t}$$

ע"פ Union Bound:

$$\Pr\left[\exists i:\left|\frac{1}{|B_i|}\sum_{x\in B_i} I(x)-\mu\right|\geq\frac{\mu}{2}\right]\leq\frac{\left(4+o(1)\right)(q-1)}{\mu t}=\frac{\left(4+o(1)\right)(q-1)}{\mu\frac{q^r-1}{q-1}}=\frac{\left(4+o(1)\right)(q-1)^2}{\mu\left(q^r-1\right)}\approx\frac{4+o(1)}{\mu q^{r-2}}$$

זה גורר:

$$\Pr\left[\exists i:\left|\frac{1}{|B_i|}\sum_{x\in B_i} I(x)-\mu\right|\geq\frac{\mu}{2}\right]\leq\frac{4+o(1)}{\mu q^{r-2}}$$

$$\Rightarrow\Pr\left[\forall i:\left|\frac{1}{|B_i|}\sum_{x\in B_i} I(x)-\mu\right|\leq\frac{\mu}{2}\right]\geq 1-\frac{4+o(1)}{\mu q^{r-2}}$$

$$\Rightarrow\Pr\left[\left|\frac{1}{|V_0+W\setminus V_0|}\sum_{x\in V_0+W\setminus V_0} I(x)-\mu\right|\leq\frac{\mu}{2}\right]\geq 1-\frac{4+o(1)}{\mu q^{r-2}}$$

$$\Rightarrow\Pr\left[\left|\frac{|(V_0+W\setminus V_0)\cap X|}{|V_0+W\setminus V_0|}-\mu\right|\geq\frac{\mu}{2}\right]=\Pr\left[\left|\frac{|(V_0+W)\cap X|}{|V_0+W|-|V_0|}-\mu\right|\geq\frac{\mu}{2}\right]\leq\frac{4+o(1)}{\mu q^{r-2}}=\frac{\left(4+o(1)\right)q^2}{\mu q^r}=\frac{\left(4+o(1)\right)q^2}{\mu|W|}$$

נספח טענות/למות/משפטים נחוצים

למה 2.2 ב [IJKW08] – Chebyshev Bound

Let $X_1,\dots,X_t$ be random variables taking values in the interval $[0,1]$, with expectation μ_i. Let $X=\sum_{i=1}^{t} X_i$ and $\mu=\sum_{i=1}^{t}\mu_i$ the expectation of X. Then for any $0<\gamma\le 1$ we have:

- *Chebyshev* – if $X_1,\dots,X_t$ are pairwise independent then $\Pr\left[|X-\mu|\ge\gamma\mu\right]\le\frac{1}{\gamma^2\mu}$

טענה 2.4 ב [IJKW08]

עבור $t=\frac{q^d-1}{q-1}$, יהיו $\alpha_1,\dots,\alpha_t\in F_q^d$ וקטורים בת"ל בזוגות. יהא A תת מרחב לינארי של U מסדר d. אזי t הוקטורים של A המתאימים ל $\alpha_1,\dots,\alpha_t$ הם בת"ל בזוגות ומתפלגים אחיד מעל U.