

PCP - Huji Course, Ex 1.

David Ponnarovsky

May 15, 2023

1 Ex 1.

Claim 1. Let A be a random matrix in $M(\mathbb{F}_2^{k \times n})$ then for any non zero $x \in \mathbb{F}_2^n$ we have that Ax distributed uniformly.

Proof. By the fact that $x \neq 0$ there exists at least one coordinate $i \in [k]$ such that $x_i \neq 0$. Thus we have

$$\begin{aligned} (Ax)_j &= \sum_k A_{jk}x_k = \sum_{i \neq k} A_{jk}x_k + A_{ji}x_i \\ &= \sum_{i \neq k} A_{jk}x_k + A_{ji} \end{aligned}$$

Notice that due to the fact that \mathbb{F}_2 is a field, there is exactly one assignment that satisfies the equation conditioned on all the values A_{jk} where $j \neq k$.

$$\Pr[(Ax)_j = 1] = \sum_{A_{jk}; k \neq i} \Pr[(Ax)_j = 1 | A_{jk}; k \neq i] \Pr[A_{jk}; k \neq i] = \frac{1}{2}$$

therefore any coordinate of Ax distributed uniformly $\Rightarrow Ax$ distributed uniformly. \square

By the uniformity of Ax we obtain that the expected Hamming weight of Ax is :

$$\mathbf{E}[|Ax|] = \mathbf{E}\left[\sum_i (Ax)_i\right] = \frac{1}{2}n$$

As the coordinates of Ax are independent (each row of A is sampled separately) we can use the Hoff' bound to conclude that:

$$\Pr\left[||Ax| - \mathbf{E}[|Ax|]| \geq \left(\frac{1}{2} - \delta\right)n\right] \leq e^{-n(\frac{1}{2}-\delta)^2}$$

Now we will use the union bound to show that any $x \in \mathbb{F}_2^k$, Ax is at weight at least δ .

$$\Pr[|Ax| \geq \delta : \forall x \in \mathbb{F}_2^k] \geq 1 - |\mathbb{F}_2^k| \cdot e^{-n(\frac{1}{2}-\delta)^2}$$

Denote $k = \rho n$ and notice that the above holds when $\rho \geq \left(\frac{1}{2} - \delta\right)^2$

2 Ex 2.

Claim 2. Let v_1, v_2, \dots, v_m unit vectors in an inner-product space such that $\langle v_i, v_j \rangle \leq -2\varepsilon$ for all $i \neq j$, then $m \leq \frac{1}{2\varepsilon} + 1$.

Proof. Let's us bound from both sides the norm of the summation $|\sum_i v_i|$. As the norm is by definition (construction) non-negative we are going to bound from the left by 0, on the other hand we have that:

$$0 \leq \left|\sum_{v_i} v_i\right|^2 = m + 2 \sum_{i,j} \langle v_i, v_j \rangle \leq m - 2 \cdot \frac{m(m-1)}{2} \cdot 2\varepsilon$$

Thus we obtain $m(2(m-1)\varepsilon - 1) \leq 0$ namely, $m \leq \frac{1}{2\varepsilon} + 1$ \square

Now, define the following product for $u, v \in \mathbb{F}_2^n$, $\langle v, u \rangle = \sum_i (-1)^{v_i} (-1)^{u_i}$ observes that:

$$1. \langle v, v \rangle = \sum_i 1 = n \geq 0.$$

$$2. \langle v, u \rangle = \langle u, v \rangle.$$

$$3. \langle ax + by, z \rangle = (-1)^a \langle x, z \rangle + (-1)^b \langle y, z \rangle.$$

Now the v 's corresponds to code with distance at least d then, i.e for any codewords v and u disagree on at least d coordinates, and therefore $\langle v, u \rangle \leq \text{agree} - \text{disagree} = n - 2 \text{disagree} = n - 2d$. Now consider the normal codewords $\tilde{v}_1, \dots, \tilde{v}_n$ and assume that $\langle \tilde{v}_i, \tilde{v}_j \rangle = (1 - 2\delta) = \frac{1}{n}(n - 2d(v_i, v_j)) \leq \varepsilon$. So if $d \geq \frac{1}{2} + \varepsilon$ we obtain the condition of the above claim.

3 Ex 3.

Consider the following process for decoding a , first we sample uniformly random $x \in \mathbb{F}_2^n$ and assign: $\hat{a}_i \leftarrow w(x) + w(\sigma_i(x))$.

Claim 3. *The above decoding returns the correct i 'th in probability greater than $\frac{1}{2}$.*

Proof. In this question we will say that w agree on $x, \sigma_i(x)$ if both $x, \sigma_i(x)$ were either flipped or unflipped. Clearly if $w(x)$ agree with $w(\sigma_i(x))$ than

$$\begin{aligned} w(x) + w(\sigma_i(x)) &= H_a(x) + H_a(\sigma_i(x)) = \sum_{i \neq j} a_j(x_j + x_j) + a_i(x_j + 1 + x_j) = a_j \text{ neither of them were flipped.} \\ &= 1 + H_a(x) + 1 + H_a(\sigma_i(x)) = a_i \text{ both flipped.} \end{aligned}$$

Also if w disagree on $x, \sigma_i(x)$ then $w(x) + w(\sigma_i(x)) = 1 + a_i$. Now consider the inner product from the above section, and observes that $\langle w(x), w(\sigma_i(x)) \rangle = 1 - (-1)^{a_i}$

□