1 Ex 1.

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

$$(Ax)_{j} = \sum_{k} A_{jk} x_{k} = \sum_{i \text{ neq}k} A_{jk} x_{k} + A_{ji} x_{i}$$
$$= \sum_{i \text{ neq}k} A_{jk} x_{k} + A_{ji}$$

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 $j \neq k$.

$$\mathbf{Pr}\left[\left(Ax\right)_{j}=1\right] = \sum_{A_{jk}; k \neq i} \mathbf{Pr}\left[\left(Ax\right)_{j}=1 \middle| A_{jk}; k \neq i\right] \mathbf{Pr}\left[A_{jk}; k \neq i\right]$$
$$= \frac{1}{2}$$

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

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

$$\mathbf{E}[|Ax|] = \mathbf{E}\left[\sum_{i=1}^{n} (Ax)_{i}\right] = \frac{1}{2}n$$

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

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

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

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

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

2 Ex 2.

Claim 2. Let $v_1, v_2..v_m$ 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 form 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:

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

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

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

1.
$$\langle v, v \rangle = \sum_{i} 1 = n \ge 0$$
.

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 $\langle v,u\rangle \leq \mathtt{agree}-\mathtt{disagree} = \mathtt{n}-\mathtt{2} \ \mathtt{disagree} = n-\mathtt{2} d.$ Now consider the normal codewords $\tilde{v_1}..\tilde{v_n}$ and assume that

$$\langle \tilde{v_i}, \tilde{v_j} \rangle = (1 - 2\delta) = \frac{1}{n} (n - 2d(v_i, v_j)) \le \varepsilon$$

So if $d \ge \frac{1}{2} + \varepsilon$ 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 grater 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 filliped or unflipped. Clearly if w(x) agree with $w(\sigma_i(x))$ than

$$\begin{split} w\left(x\right) + w\left(\sigma_{i}(x)\right) &= H_{a}(x) + H_{a}(\sigma_{i}(x)) \\ &= \sum_{i \neq j} a_{j}(x_{j} + x_{j}) + a_{i}(x_{j} + 1 + x_{j}) = a_{j} \text{neither of them were flipped.} \\ &= 1 + H_{a}(x) + 1 + H_{a}(\sigma_{i}(x)) = a_{i} \text{both flipped.} \end{split}$$

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 $\langle w(x), w(\sigma_i(x)) \rangle = 1 - (-1)^{a_i}$