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

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

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 $j \neq k$.

$$
\begin{aligned}
\mathbf{Pr}\left[(Ax)_j = 1\right] &= \sum_{A_{jk}; k \neq i} \mathbf{Pr}\left[(Ax)_j = 1 | A_{jk}; k \neq i\right] \mathbf{Pr}\left[A_{jk}; k \neq i\right] \\
&= \frac{1}{2}
\end{aligned}
$$

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

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

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

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

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

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

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

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

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:

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

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

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

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 $\langle v, u \rangle \leq \texttt{agree} - \texttt{disagree = n - 2 disagree}$ $= n - 2d$. Now consider the normal codewords $\tilde{v}_1..\tilde{v}_n$ and assume that

$$\langle \tilde{v}_i, \tilde{v}_j \rangle = (1 - 2\delta) = \frac{1}{n}\left(n - 2d(v_i, v_j)\right) \leq \varepsilon$$

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,

```
1  for t ∈ [τ] do
2      for i ∈ [n] do
3          x ∼ᵤ 𝔽₂ⁿ
4          aᵢ⁽ᵗ⁾ ← w(x) + w(σᵢ(x))
5      end
6  end
7  for i ∈ [n] do
8      âᵢ ← [1/τ ∑ₜᵀ aᵢ⁽ᵗ⁾]
9  end
10 return â₀, â₁, â₂..âₙ
```

Claim 3. *For* $\tau = \Omega\left(\frac{1}{\varepsilon^4}\log(n)\right)$ *The above decoding success to decode* $w(x)$ *with probability* $\geq 1 - \frac{1}{n}$.

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

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

Thus we can bound the probability that $w(x) + w(\sigma_i(x)) \neq a_i$ by the probability that w disagree on x and that append at probability:

$$\xi := (1 - f(x))f(\sigma_i(x)) + (1 - f(\sigma_i(x)))f(x)$$

Now as we want bound ξ we could think about the maximization problem under the restrictions that $f(x), f(\sigma_i(x) \leq \frac{1}{2} - \varepsilon$. We know that the maximum lay on the boundary so we can assign $\frac{1}{2} - \varepsilon$ for each of the probabilities to obtain an upper bound. That will yield $\xi \leq 2 \cdot \left(\frac{1}{2} - \varepsilon\right)\left(\frac{1}{2} + \varepsilon\right)$, namely $\xi \leq \frac{1}{2} - 2\varepsilon^2$. Now the probability that a coordinate i will rounded to the opposite side, that it $\hat{a}_i \neq a_i$ mean that arithmetic mean over τ experiments were $2\varepsilon^2$ far from the expectation. Which by Hoff' bound is bounded by: $e^{\tau 4\varepsilon^4}$. So using the union bound we obtain:

$$\mathbf{Pr}\left[\text{ decoding success }\right] \geq 1 - n \cdot e^{\tau 4\varepsilon^4}$$

Therefore it's enough to take $\tau = O(\frac{1}{\varepsilon^4}\log(n))$ to obtain a decoder which run at time $O(\frac{1}{\varepsilon^4}n\log(n))$ and success with heigh probability. $\qquad \square$

4 Ex 4.

4.1 (a)

We will prove that if for any x, f interpolate well on $x, x+1, .., x+d+1$ than any it interpolate well on every coordinates set at size $d+1$. Denote by $J \subset \mathbb{F}_q$ at size $d+1$. Let's continue by induction on $\max J$. The base case $\max J = d+1 \Rightarrow J = \{1, 2.., d+1\}$ follow straightforwardly from the assumption. Assume the correctness for any J such that $\max J \leq x_0$ and consider J' such that $\max J' = x_0+$. Now it given that $S = \{x_0 - d, x_0 - d + 1, ..x_0 + 1\}$ is well interpolating set, so there exists coefficients a_1, a_{d+1} such that $a_{d+1} f(x_0 + 1) = \sum_{x_i \in S/(x_0+1)} a_i f(x_i)$ On the overhand, for ant any $x_i \in S/(x_0 + 1)$ the union $K = x_i \cup J/(x_0 + 1)$ is subset of $\mathbb{F}_q$ at size $d+1$ such that $\max K \leq x_0$. Hence by induction assumption K is well interpolating set and we can exchange any $f(x_i)$ for $x_i \in S$ by a linear combination of $f(x_i)$ for $x_i \in J/(x_0 + 1)$. So in overall we obtain that J is depended set, namely f is well interpolate on J.

4.2 (b)

Define the function $g(x) = f(t^{-1}(x - s))$. Note that q is prime, thus $(\mathbb{F}_q/0, \cdot)$ and $(\mathbb{F}_q, +)$ are groups and the inverse elements $-s, t^{-1}$ are exist and uniqs. Suppose that y is a zero of $g \Rightarrow f(t(y + s)) = g(y) = 0$, Hence the number of zeros of f equals to the number of zeros of g, which means that their degree are equal $\Rightarrow g$ is also a polynomial at degree at most d, $\Rightarrow a_1, a_2..a_d$ are also the interpolation coefficients respecting to the interpolation set $\{tx_1 + s, tx_2 + s, .., tx_d + s\}$.

5 Ex (5).

5.1 (a)

As shown in the above section, by the fact that q is prime we have that $g_{v,u}$ act on $\mathbb{F}_q^m$ by $g_{u,v}(x) = v + ux$, (for any $u \neq 0$) Thus $f(g_{u,v}(x))$ is just a permutation over the values of f. As the number of zeros remain the same, we have that $f(g_{u,v}(x))$ is also degree d polynomial. Thus the restircted polynomail $f|_L$ correspond to restriction L_I of another polynomial obtained by taking $v' = 0$ and u to be supported only on single coordinate. Hence the restricted polynomial can has at most d zeros.

5.2 (b)