Lecture 4 :- Brief review of $\mathbb{F}_{2^d}$.

$\mathbb{F}_2[x]$: all polynomials with coefficients in $\mathbb{F}_2$.

Irreducible polynomials in $\mathbb{F}_2[x]$

A polynomial $p(x) \in \mathbb{F}_2[x]$ of degree $d > 1$ is irreducible if there are no polynomials $g(x), h(x) \in \mathbb{F}_2[x]$ of degree strictly less than d s.t.

$$p(x) = g(x)\, h(x).$$

(just as in integers).

Implies :- If $p(x) \in \mathbb{F}_2[x]$ is irreducible and $q(x) \in \mathbb{F}_2[x]$ is such that $p(x)$ does not divide $q(x)$, then there exists $r(x) \in \mathbb{F}_2[x]$ s.t.

$$q(x) \cdot r(x) = 1 \mod p(x).$$

$$\left(q(x) \cdot r(x) = 1 + p(x)\, s(x) \text{ for some } s(x) \in \mathbb{F}_2[x] \right)$$

So we define

$\mathbb{F}_{2^d} := \mathbb{F}_2[x]/p(x)$ where $p(x) \in \mathbb{F}_2[x]$ is an irreducible polynomial of degree d.

$= \{ q(x) \in \mathbb{F}_2[x],\ \deg(q) < \deg(p) \}$ addition, multiplication and inversion defined modulo p }.

[**Theorem** (we won't prove) : There is exactly one field of size p^d (p prime, $d \geq 1$), upto isomorphism]

Examples :- x^2+1 is irreducible in $\mathbb{R}[x]$.

is not irreducible in $\mathbb{C}[x]$ $(x+i)(x-i)$.

is not irreducible in $\mathbb{F}_2[x]$.

$(x^2+1 = (x+1)(x+1) = x^2+1$ in $\mathbb{F}_2[x]$.)

$x^2 = x \cdot x$. not irreducible.

$x^2+x = x(x+1)$ " "

x^2+x+1 : irreducible. (Check that x does not divide $p(x)$, neither does $x+1$).

Theorem:- There exist irreducible $p(x) \in \mathbb{F}_2[x]$ of every degree $d \geq 1$.

Coming back to AMS:- we will choose [once!] an irreducible polynomial of degree $d = \lceil \lg D \rceil$, and use the k-wise independence construction over $\mathbb{F}_{2^d}$ using this polynomial. [Each element is now represented as the coefficient bit-vector (of dimension d) of a degree $d-1$ polynomial over $\mathbb{F}_2$.]

We get 4-wise independent d-length bit vectors, each of which as the uniform distribution over $\{0,1\}^d$. To make them our bits, take parity / fixed index.

Remark:- Note that D can be less than $\mathbb{F}_{2^d}$. The construction gives us $|\mathbb{F}_{2^d}| = 2^d$ uniformly random 4-wise independent signs, We just ignore $2^d - D$ of these signs.

Now:- We had $sk = O\left(\frac{1}{\varepsilon^2}\log(1/\delta)\right)$ counters, for each of which we needed a vector of D 4-wise independent uniformly random signs. [The vectors for different counters were independent].

So for each counter we need to store $\vec{z} \in \mathbb{F}_{2^d}^4$ (chosen independently uar, across counters). This requires $4 \cdot d = 4\lceil \log D \rceil = O(\log D)$ storage per counter.

Total randomness storage = $sk \cdot O(\log D)$

$$= O\left(\frac{\log D \log(1/\delta)}{\varepsilon^2}\right)$$

We if we a total of n elements, each counter needs only $O(\log n)$ bits. So we get a total Storage of

$$O\left(\frac{\log(1/\delta)}{\varepsilon^2}\left(\log n + \log D\right)\right)$$

No linear dependence on D!!

Computation per new element: Each of the sk counters has to be updated. Each counter update requires an evaluation of a degree-4 polynomial over $\mathbb{F}_{2^d}$ taking time $O(d^2)$. Update time guarantee is also of the form:

$$O(sk \cdot \text{poly}(d))$$

$$= O\left(\frac{1}{\varepsilon^2} \log(1/\delta) \cdot \text{poly log}(D)\right).$$

arithmetic operations.

From looking at the code

- Even the theoretical bound warns about a bad dependence on $1/\varepsilon^2$ on the update time per item [unless counters are parallel :]
- Implementations matter: A properly optimized implementation of the field arithmetic could do much better.

Hoeffding bound for bdd. random variables:-

(We used this but never proved it.)

Thm: Let X be a mean zero random variable taking values in $[a, b]$. $(a \leq 0 \leq b)$.

Then $\psi_X(\lambda) := \log E[\exp(\lambda X)]$ satisfies

$$\psi_X(\lambda) \leq \frac{(b-a)^2 \lambda^2}{8}.$$

Proof:-

$$\psi_X(0) = 0.$$

$$\psi_X'(\lambda) = \frac{E[X \exp(\lambda X)]}{E[\exp(\lambda X)]}$$

(Assuming Measure theoretic conditions for differentiating under the integral).

$$= E_{\mu_\lambda}[X]$$

(What this means:- We define.

$$E_{\mu_\lambda}[Z] := \frac{E[Z \exp(\lambda X)]}{E[\exp(\lambda X)]}.$$

μ_λ is a probability distribution:

$$E_{\mu_\lambda}[1] = 1.$$)

$$\psi_X'(0) = \frac{E[X]}{1} = 0. \quad (\because X \text{ was zero mean})$$

$$\psi_X''(\lambda) = \frac{E[X^2 \exp(\lambda X)]}{E[\exp(\lambda X)]} - \frac{E[X \exp(\lambda X)]^2}{E[\exp(\lambda X)]^2}.$$

$$= E_{\mu_\lambda}[X^2] - E_{\mu_\lambda}[X]^2.$$

$$= \mathrm{Var}_{\mu_\lambda}(X).$$

$$= E_{\mu_\lambda}\left((X - E_{\mu}(X))^2\right) \quad (\leq (b-a)^2). \quad \text{Clearly.}$$

$$= \min_{t \in \mathbb{R}} E_{\mu_\lambda}\left[(X-t)^2\right]$$

$$\leq E_{\mu_\lambda}\left[\left(X - \frac{b+a}{2}\right)^2\right]$$

$$\leq E_{\mu_\lambda}\left[\left(\frac{b-a}{2}\right)^2\right] \quad (\because X \in [a,b]$$

$$= \frac{(b-a)^2}{4}.$$

$$\psi_X(0) = 0$$

$$\psi_X'(0) = 0$$

$$\psi_X''(\lambda) \leq \frac{(b-a)^2}{4}. \quad -(1)$$

By Taylor theorem with the second order era tem we have; $\forall \lambda \in \mathbb{R}$, $\exists \mu \in \mathbb{R}$ s.t $(\mu \in \text{seg}[0,\lambda])$

$$\psi_X(\lambda) = \psi_X(0) + \psi_X'(0)\lambda + \frac{\psi_X''(\mu)\lambda^2}{2}.$$

$$= \frac{\psi_X''(\mu)\lambda^2}{2}$$

$$\leq \frac{(b-a)^2\lambda^2}{8}. \quad \text{from } (1).$$