Lecture 16

Sketches (AMS)

for every $i \in [n]$ $\{1, \dots, n\}$

$f(i) = \sum_j f_{ij}^2 = F_2$

f_i is F_2 in column i

$X = \sum_i f_i \xi_i$

$Z = X^2$

$E(Z) = F_2$ ξ_i 2-wise indep

$\mathrm{Var}(Z) \le 2F_2^2$

$\mathrm{Var}(Z) = E(Z^2) - E(Z)^2$ 4-wise indep

$\le 3F_2^2 \quad F_2^2$

Chebyshev bound

$$P\left(|Z - F_2| > \sqrt{\mathrm{Var}(Z)}\right) \le \frac{1}{\gamma^2}$$

$\varepsilon(t)$

$$P(|X - E[X]| > \varepsilon) \le \frac{V_2(X)}{\varepsilon^2}$$

$$P\left(|Z - F_2| > \gamma\sqrt{2}\, F_2\right) \le \frac{1}{\gamma^2}$$

ξ_i: relative error ε_2

$\gamma = \frac{\varepsilon_2}{\sqrt{2}\varepsilon_1}$ $P(\text{off by rel. error } \varepsilon_1) \le \frac{2}{\varepsilon_1^2}$

Assume $t_1, \dots, t_m$ indep replicates of Z

$\hat{Z} = \frac{\sum t_i}{m}$

$V_2(\hat{Z}) = \frac{V_2(Z)}{m}$

Generation of z_i

$$z_i = F(i, S)$$

(S ← seed)

Seed $2n$ random bits

$$F(i, S) = S(i)$$

2-wise indep

S of n bits

$|I| = 2^n$

n-bit seq

z_i's

$F(i, S) =$ 2-wise indep

$\langle i, S\rangle$ – dot product over vector space of size n over $GF(2)$ — **Galois Field.**

$GF(2)$ $\{0, 1\}$

$+$ XOR

$*$ AND

$$\langle i, S\rangle = i_1 S_1 \oplus i_2 S_2 \oplus \dots \oplus i_n S_n$$

i_j – jth bit of i

S_j — || — of S

0 1

Pairwise independence

$\forall\, i_1 \neq i_2$

$\{_{i_1}$ is in any of $\{_{i_2}$

$\langle i_1, S\rangle$, $\langle i_2, S\rangle$ are in any

$P[\{_{i_1} = \cdot\,' \;/\; \{_{i_2} = \cdot\,'] = \frac{1}{2}$

$= \frac{1}{2}$

$= \frac{1}{4}$

6) bits indexed by i_1'th bits

$\leftarrow$ bit

$\widehat{f}(i_1) = r_0 \oplus \langle i_1, S_1\rangle \oplus \langle i_2, S_2\rangle$

2^{n-1}

$\Pr_S[\langle i_1, S\rangle = 0 \wedge \langle i_2, S\rangle = 0] = \frac{1}{4}$

(and for all pairs i_1, i_2 and a, b)

S	$\langle i_1, S\rangle$	$\langle i_2, S\rangle$
0 0 0 0	0	0
0 0 0 0 1	0	0
0 0 0 1 0	0	1
0 0 0 1 1	0	1
0 0 1 0 0	1	0
0 0 1 0 1	1	0
0 0 1 1 0	1	1
0 0 1 1 1	1	1
...	...	...

$0 \oplus 0 = 0$

$0 \oplus 1 = 1$

$1 \oplus 0 = 1$

$1 \oplus 1 = 0$

PRF code

$\widehat{S}(i, S) = r_0 \oplus \langle i_1, S_1\rangle \oplus \ldots \oplus \langle i^{k}, S_k\rangle$

$S = [r_0, S_1, \ldots, S_k]$ — $n(k+1)$ bits

$(k+1)$ independent $\{_i$'s

(i_0 computed in finite field)

Seeds produced from
Mahmood

Mahmood by Sitan