

Now use the usual representation of $GF(2^r)$ by the coefficients of polynomials of degree $\leq r-1$ over $GF(2)$, modulo an irreducible of degree r .

$$M_2 = \begin{bmatrix} 001 & a_1 = 001 & a_1^2 = \dots & a_1^{k-1} = 001 \\ 001 & 010 & & \\ \vdots & \vdots & & \\ 001 & a_n = 111 & a_n^2 = \dots & a_n^{k-1} \end{bmatrix} \quad \begin{array}{l} \text{matrix} \\ \text{over} \\ GF(2) \end{array}$$

Every k rows of M_2 are linearly independent over $GF(2)$.

Further reduce the number of columns:

1. Drop leading 0's in first entry.

2. Strike out all positive-even-power columns.

$$M_3 = \begin{bmatrix} | & a_1 & a_1^3 & \dots \\ | & a_2 & a_2^3 & \dots \\ \vdots & \vdots & \vdots & \\ | & a_n & a_n^3 & \dots \end{bmatrix} \quad \begin{array}{l} \text{matrix} \\ \text{over} \\ \text{GF}(2) \end{array}$$

Claim: Every set of rows independent in M_2 ,
is also independent in M_3 .

Hence every k rows of M_3 are independent.

Pf:

Let $\{i_1, \dots, i_{c_1}\}$ be a set of independent rows
in M_2 . Then any subset of these, say $\{i_1, \dots, i_{c_2}\}$, sums to
nonzero
vector.

Let $2t > 0$ be the least positive even power
for which $\sum_{j=1}^{c_2} a_{i_j}^{2t} \neq 0$.

Since characteristic = 2, $\sum_j a_{i_j}^{2t} = \left(\sum_j a_{i_j}^t\right)^2$

hence $\sum_j a_{i_j}^t \neq 0$.

$\Rightarrow t$ odd \Rightarrow Rows $\{i_1, \dots, i_{c_2}\}$ have nonzero sum in M_3 .

\Rightarrow Rows $\{i_1, \dots, i_{c_1}\}$ are independent in M_3 .

Recalling $n = 2^r - 1$,

$$|S| = 2^l = 2^{1+r \lfloor k/2 \rfloor} \approx n^{\lfloor k/2 \rfloor}.$$

Lower Bound:

If z_1, \dots, z_n are k -wise independent random variables* then $|S|$ is $\Omega(n^{\lfloor k/2 \rfloor})$.

* not a.s. constant

Thm: Let

$$m(n, k) = \begin{cases} \sum_{j=0}^{k/2} \binom{n}{j} & (k \text{ even}) \\ \binom{n-1}{\frac{k-1}{2}} + \sum_{j=0}^{\frac{k-1}{2}} \binom{n}{j} & (k \text{ odd}) \end{cases}$$

Then: $|S| \geq m(n, k)$.

pf: Relabel the values taken by each z_i
by subtracting $E(z_i)$,
so that for all i , $E(z_i) = 0$.

Now for any $S \subseteq \{1, \dots, n\}$ define the
random variable d_S by

$$d_S = \prod_{i \in S} z_i$$

k -wise independence implies:

$$E(d_S d_T) = \begin{cases} \text{positive} & \text{if } S = T \text{ and } |S| \leq k \\ 0 & \text{if } S \neq T \text{ and } |S \cup T| \leq k \end{cases}$$

Let \mathcal{J} be following set system:

If k is even:

$$\mathcal{J} = \left\{ S \subseteq \{1, \dots, n\} : |S| \leq k/2 \right\}$$

If k is odd:

$$\mathcal{J} = \left\{ S : |S| \leq \frac{k-1}{2} \right\} \cup \left\{ S : |S| \leq \frac{k+1}{2} \text{ AND } 1 \in S \right\}$$

$$\Rightarrow |S \cup T| \leq k \quad \forall S, T \in \mathcal{J}.$$

$$|\mathcal{J}| = m(n, k).$$

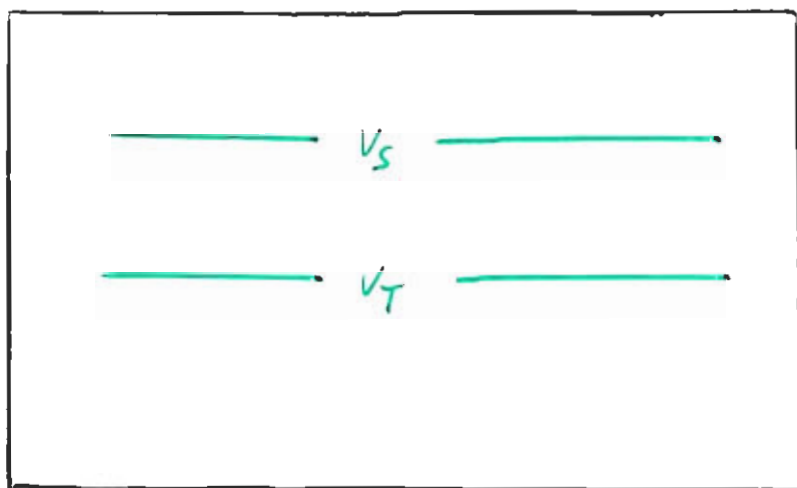
For $S \in \mathcal{J}$, let v_S be the vector $v_S \in \mathbb{R}^{|S|}$

$v_S(i)$ = the value of α_S on the i^{th} point

of the sample space S , $\times \sqrt{p(i)}$

(where $p(i)$ = Probability of the i^{th} sample point)

$m(n, k)$



$|S'|$

$$E(d_S, d_T) = \text{[blacked out]} v_S \cdot v_T$$

\Rightarrow The rows are orthogonal

$\Rightarrow |S'| \geq m(n, k)$.