Polynomial evaluation.

q prime / prime power

$\mathbb{F}_q = \{0, 1, \ldots, q-1\}$ operations mod q.

n - degree of polynomial.

Data: $P(X) \in \mathbb{F}_q[X]$

$\deg(P) \leq n$.

Queries: $x \in \mathbb{F}_q$.

Answer: $P(x)$.

Word size = $O(\log q)$.

$q = n^3$ is a good setting.

2 trivial data structures

1. Store coeffs of $P(X)$
   $O(n)$ words of space — OPTIMAL
   $O(n)$ query time.

2. Store values of $P(X)$
   $O(q)$ words of space
   $O(1)$ query time — OPTIMAL.

Thm Any data structure for poly evaluation with w-bit words for $w = O(\log q)$ ~~needs~~ and $O(n)$ space needs $\Omega(\log n)$ query time.
[Larsen '12] [Siegel '04]

Proof Suppose there was a data structure with s words of space, and t query time.

Let $p \in [0, 1]$, some parameter.
Independently, for each ~~cell~~ cell of memory, we keep the cell with probability p, and destroy it w.prob. $1-p$.

Expect about $p^t \cdot q$ queries to be answerable with this corrupted data structure.

If $p^t \cdot q > n+1$, then we expect have enough information in the corrupted data structure to recover $P(X)$.

FISHY [But this is $p \cdot s$ words of space.

$= psw$ bits of space.]

$$\boxed{\begin{array}{l}\text{Need } psw > n \log q \\ \text{if } p^t \cdot q > n+1\end{array}}$$

[Simple calculation:

$w = O(\log q)$ $\quad q = n^3$

$t = \underline{c \log n}$.

$p = 2^{1/\epsilon}$.

$\Rightarrow s \geq \Omega(\underline{2^{1/\epsilon}} \cdot n)$

$s \geq n^{O(\frac{1}{\epsilon})} \cdot n$

If there was such a data structure, let us use it to encode a $\deg n$ polynomial with $< n \log q$ bits.

1. Find a set U of $\underline{ps}$ cells of memory s.t. $\geq p^t \cdot q$ queries can be answered using it.

2. Write down (a) the set U

   (b) the contents of the memory cells in U.

(a) $\rightarrow \leq s$ bits.

(b) psw bits.

Total # bits written down $\leq s + psw$.

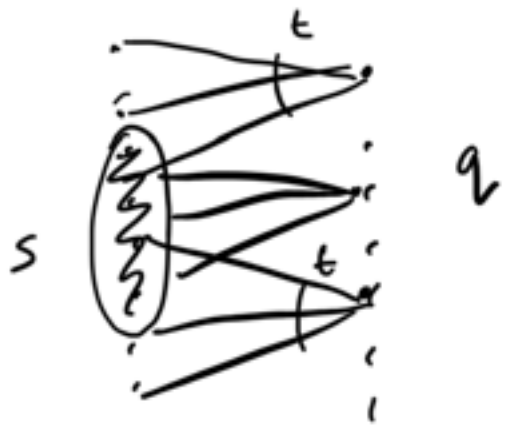
If $\underbrace{s}_{} + psw < (n+1) \log q$, we have a contradiction

---

A collection $A_1 \ldots A_q$ of subsets of $\{1, 2, \ldots s\}$, each subset of size $\leq t$.

<u>Claim</u> $\exists\ U \subseteq \{1, \ldots, s\}$ s.t.

$\#i : A_i \subseteq U$ is $\geq p^t \cdot q$.



If we pick ps cells U uniformly at random then for each A_i, let $X_i = 1$ if $A_i \subseteq U$.

$$\mathbb{E}[X_i] = \frac{\binom{s-t}{ps-t}}{\binom{s}{ps}}$$

$$E\left[\sum X_i\right] = \sum E[X_i]$$

$$= q \cdot \frac{\binom{s-t}{ps-t}}{\binom{s}{ps}}$$

$$= q \cdot \frac{\dfrac{(s-t)!}{(ps-t)!\,\cancel{(s-ps)!}}}{\dfrac{s!}{(ps)!\,\cancel{(s-ps)!}}}$$

$$= q \cdot \frac{(ps)\cdot(ps-1)\cdots(ps-t+1)}{s\,(s-1)\cdots(s-t+1)}$$

$$\approx q \cdot p^t \cdot \left(1-\frac{t}{ps}\right)^t$$