$P_d = \{ f : \mathbb{F}_2^* \rightarrow \mathbb{F}_2 | \deg (f) \leq d \}$

Want to test with few queries whether:
(a) $f$ is degree-$d$ polynomial ($f \in P_d$), or
(b) $f$ far from all degree-$d$ polynomials ($\delta (f, P_d) \geq \text{some constant } \delta$)

**Basic test $Test_k (k$-flat test)**

- Pick random $k$-flat $A \subseteq \mathbb{F}_2^n$ (affine subspace of dimension $k$)
- Reject if $f \nmid A$ not degree-$d$ polynomial

$Rej_{k, f} = \text{rejection probability of } Test_k$ for $f$

$k$-flat $A \subseteq \mathbb{F}_2^n$ is
\[ A = \{ Mx + b | x \in \mathbb{F}_2^k \} \]

for some full-rank $M \in \mathbb{F}_2^{n \times k}$ and some $b \in \mathbb{F}_2^n$

**Hyperplane:** $(n - k)$-flat

**Question:** What does it mean, actually, that $f \nmid A$ is a degree-$d$ polynomial?

**Let $M = (m_{ij})$**

Suppose we have $f (y_1, \ldots, y_n)$

Define $g(x_1, \ldots, x_k) = f (y_1, \ldots, y_n)$ for
\[ y_i = \sum_{j=1}^{k} m_{ij} x_j + b_i; \quad f \nmid A = g \]
**Main Theorem [BKSSZ 10]**

\[ \exists \epsilon > 0 \text{ s.t. } \forall d, n \in \mathbb{N}^+, f: \mathbb{F}_2^n \to \mathbb{F}_2, \text{ it holds that} \]

\[ \text{Reg}_{d+1}(f) \geq \min\{2^d, \delta(f, P_d), \epsilon\} \]

**Corollary**

Testing of degree-d polynomials doable with \(O(2^d + \sqrt{d})\) queries (and this is optimal)

The analysis of the \(k\)-flush test goes as follows.

\[ \boxed{A} \]

If \( f \) is really close to \( P_d \) but not an \( P_d \), then \( \text{Reg}_{d+k}(f) \geq \delta(f, P_d) \) for any \( k \) (and we're in good shape).

The idea here is that with good probability the flat will contain exactly one point where \( f \) and closest \( P \in P_d \) differ, and so \( f \) will be rejected.

\[ \boxed{B} \]

If \( k \geq d + 10 \), then \( T_{d+1} \) rejects \( f \) with constant probability. If \( \delta(f, P_d) = 2(2 - d) \)

In some sense, the tester is good enough to provide us some slack here.

\[ \boxed{C} \]

The tester \( T_{d+1} \) can't be much worse than \( T_{d+k} \) for \( k \geq d + 2 \), and using the slack from \( B \) this can take us down from dimension \( d+10 \) to \( d+1 \).
**Lemma A**

For every \( k, l, d \in \mathbb{N}^+ \) such that \( k > l > d+1 \), if \( \delta(f, P_d) = \delta \)
then
\[
\text{Rej}_{d+1}(f) \geq 2^d \delta (1 - (2^d - 1) \delta).
\]

In particular, if \( \delta \leq 2 - (d+2) \), then
\[
\text{Rej}_{d+1}(f) \geq \min \{ \frac{1}{8}, 2^{k-1} \cdot \delta \}\]

**Lemma B** (Key Lemma)

There exist positive constants \( \beta < 1/4 \), \( \epsilon_0 > 0 \), and \( c \)
such that the following holds for every \( d, k, n \in \mathbb{N}^+ \) such that \( n \geq k \geq d+c \):

Let \( f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \) be such that
\[
\delta(f, P_d) \geq \beta \cdot 2^{-d}. \text{ Then}
\]
\[
\text{Rej}_{d+1}(f) \geq \epsilon_0 + \gamma \cdot 2^{d/2-n}.
\]

**Lemma C**

For every \( d, k, h, n \in \mathbb{N}^+ \) such that \( n \geq k \geq d+1 \) and every \( f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \)

it holds that
\[
\text{Rej}_{d+1}(f) \geq \text{Rej}_{d+h}(f) \cdot 2^{-h(-k-k')}
\]
We need to talk a bit more about hyperplanes $A, B \in \mathbb{F}_2^n$ are complementary hyperplanes if $A \cup B = \mathbb{F}_2^n$

Not hard to verify that any hyperplane can be described as set of points

$$\{ x \in F_2^n \mid \ell_c(x) = 6 \}$$

for some $\ell_c(x) = \sum_{i=1}^n c_i x_i = \langle c, x \rangle$ for $c \in \mathbb{F}_2^n$, $c \neq 0$

Refer to $\ell_c$ as linear part of hyperplane

We say that hyperplanes $A_1, \ldots, A_e$ are linearly independent if the corresponding linear parts are linearly independent (i.e., the vectors $c$ for the $\ell_c$ are independent)

**Proposition 1** (Properties of hyperplanes)

1. There are exactly $2^{n+1} - 2$ distinct hyperplanes in $\mathbb{F}_2^n$

2. Among any $2^e - 1$ distinct hyperplanes there are at least $e$ independent hyperplanes

3. There is an affine invertible transform that maps linearly independent hyperplanes $A_1, \ldots, A_e$ to the hyperplanes $x_1 = 0, \ldots, x_e = 0$

   [i.e., $M \in \mathbb{F}_2^{n \times n}$ full-rank, $t \in \mathbb{F}_2^n$, such that $x \in \mathbb{F}_2^n$ is sent to $y = Mx + t$]

*Proof Exercise.*
Proof of Lemma A: "If $f$ close to $P_d$, we're good."

In one line: With good probability a random flat will contain exactly one point where $f$ and closest degree-$d$ polynomial disagree, which will cause test to reject.

We will prove

$$
\text{Rej}_{d,k}(f) \geq 2^k \delta (1 - (2^k-1)\delta)
$$

(All such claims will have proofs left as exercises)

If $k \geq \ell$, then $\text{Rej}_{d,\ell}(f) = \text{Rej}_{d,k}(f)$

(looking at larger subspace can never hurt.)

Given (1) and CLTM(i), second part follows

Namely, assume $\delta(f, P_d) = \delta \leq 2^{-(d+2)}$

If $\delta \leq 2^{-(\ell+1)}$, set $\ell = \ell$

Otherwise, choose $\ell$ such that $2^{-(\ell+1)} < \delta \leq 2^{-(\ell+2)}$

(which is possible since $\delta \leq 2^{-(d+2)}$)

Former case:

$$
\text{Rej}_{d,k}(f) \geq 2^k \delta (1 - (2^k-1)\delta)
$$

$$
\geq 2^k \delta (1 - 2^k \delta)
$$

$$
\geq 2^k \cdot \delta \cdot (1 - \frac{1}{2})
$$

$$
= 2^{k-1} \delta
$$

Latter case:

$$
\text{Rej}_{d,k}(f) \geq 2^\ell \delta (1 - (2^\ell-1)\delta)
$$

$$
\geq 2^\ell \cdot 2^{-(\ell+1)} (1 - 2^\ell \cdot 2^{-(\ell+1)})
$$

$$
= 2^{-2} \cdot (1 - \frac{1}{2}) = \frac{1}{8}
$$
Let $M \in \mathbb{F}_2^{n \times l}$ random full-rank matrix
Let $b \in \mathbb{F}_2^l$ random
Denote

$$a_x = Mx + b$$

Then the random $\ell$-flat $A$ is

$$A = \{ a_x \mid x \in \mathbb{F}_2^l \}$$

Let $g \in \mathcal{P}_d$ be such that $\delta(f, g) = 5$
Define events

$$E_x = \text{"} f(a_x) \neq g(a_x) \text{"}$$

$$F_x = \text{"} f(a_x) \neq g(a_x) \text{ and } \forall y \neq x \ f(a_y) = g(a_y) \text{"}$$

If any $F_x$ occurs, then $T(x)$ rejects
This is because distinct degree-$d$ polynomials differ in at least a $2^{-d}$ fraction of points
[ Lecture 9, page 311 ]
So no two degree-$d$ polynomials can disagree in a single point in $\ell > d$.

Claim (ii)
For $x, y \in \mathbb{F}_2^l$, $x \neq y$, then for random $M$ and $b$ as above, $a_x$ is distributed uniformly over $\mathbb{F}_2^l$ and $a_y$ is distributed uniformly over $\mathbb{F}_2^l \setminus \{a_x\}$
Hence (with probabilities over choice of $M$ and $E$, i.e., of random $L$-flat):

\[ \Pr [E_x] = \delta \]

\[ \Pr [E_x \text{ and } E_y] = \Pr [E_x] \cdot \Pr [E_y | E_x] \leq \delta \cdot \delta = \delta^2 \]

From this we get

\[ \Pr [F_x] = \Pr [E_x \setminus \bigcup_{y \neq x} (E_x \cap E_y)] \]

\[ \geq \Pr [E_x] - \sum_{y \neq x} \Pr [E_x \text{ and } E_y] \]

\[ \geq \delta - (2^t - 1) \delta^2 \]

\[ = \delta (1 - (2^t - 1) \delta) \]

Since events $F_x$ are mutually exclusive, we obtain

\[ \text{Reject}(f) \geq \Pr [U_x F_x] \]

\[ = \sum_x \Pr [F_x] \]

\[ \geq 2^t \delta (1 - (2^t - 1) \delta) \]

and Lemma 4 follows.
Proof of Lemma C

"If for \( k \geq k' \), \( k' = k - o(1) \), \( k \)-flat test good, then \( k' \)-flat test must also be fairly good."

Need Proposition 1 and two lemmas.

**Lemma 2**

Let \( k \geq d + 1 \) and suppose \( f : \mathbb{F}_2^{(k+1)} \rightarrow \mathbb{F}_2 \) has degree \( \deg(f) > d \). Then

\[ \text{Reg}_d(f) > \frac{1}{2} \]

**Proof** By contradiction. Suppose not.

Means that on strict majority of hyperplanes \( A \) \( f \mid A \) has degree \( d \).

In particular, exist complementary hyperplanes \( A, A \) \( f \mid A, f \mid A \) both degree-\( d \) polynomials, say \( g_A : \mathbb{F}_2^{k} \rightarrow \mathbb{F}_2 \) \( g_A : \mathbb{F}_2^{k} \rightarrow \mathbb{F}_2 \).

If for a matrix \( M \in \mathbb{F}^{n \times k} \) has full column-rank \( (n \geq k) \), then there exists a pseudoinverse \( M^+ \in \mathbb{F}^{n \times k} \) such that

\[ M^+ M = I \]

Suppose \( A = \{ Mx + b \mid x \in \mathbb{F}_2^{n \times (n-1)} \} \)

Then for a point \( a \in A \) (as in (2)) we have
\[ a_x = Mx + b \]

\[ M^+ a_x = x + M^+ b = x + b^+ \]

i.e. we can express \( x \in \mathbb{F}_2^{n-1} \) in terms of \( y \in \mathbb{F}_2^n \) as

\[ x = M^+ y + b^+ \]

and this map is bijective for \( y \) restricted to \( A \)

In this way, from \( g_A \in \mathbb{F}_2[X_1, \ldots, X_{n-2}] \)
we obtain a polynomial \( p_A \in \mathbb{F}_2[y_1, \ldots, y_{n-2}] \)
by

\[ p_A(y) = g_A(M^+ y + b^+) \]

such that \( \deg(p_A) \leq d \) and

\[ \forall y \in A \quad f(y) = p_A(y) \]

Construct \( p_A^-(y) \) in the same way.

Suppose (using (x))

\[ A = \{ y \in \mathbb{F}_2^n \mid \lambda(y) = 0 \} \]

\[ \overline{A} = \{ y \in \mathbb{F}_2^n \mid \lambda(y) = 1 \} \]

Then

\[ p_{\lambda y}(y) = (\lambda(y) - 1) p_A(y) + \lambda(y) \cdot p_{\overline{A}}(y) \]
is a polynomial of degree \( d + 1 \)
that equals \( f \) everywhere, i.e. \( f = P \).

If \( \deg(P) \leq d \), we get a contradiction.

Hence suppose \( \deg(P) = d + 1 \).

Since \( \text{Re}(f(x)) < \frac{1}{2} \), on a strict majority of hyperplanes \( A \) we have that \( f \cap A = P \cap A \) has degree \( d \).

Strict majority means (by Proposition 1(1)) at least
\[
\frac{1}{2} \left( 2^{k+2} - 2 \right) + 1 > 2^{k+1} - 1
\]
hyperplanes, i.e., (by Proposition 1(2)) at least \( k + 1 \geq d + 2 \) linearly independent hyperplanes \( A_1, \ldots, A_{d+2} \).

Claim (iii)

Let \( y = Mx + b \) full-rank affine transform on \( \mathbb{F}_2^n \). Let \( A(x) = P(Mx + b) \).

Then \( \deg(A) = \deg(P) \).

Using this and Prop 1(3), we can assume that the hyperplanes are
\( x_1 = 0, \ldots, x_{d+2} = 0 \).
Using (1) again, we see that

\[ f_n(x_i) = P_n(x_i) = P(x_1, \ldots, x_n) |_{x_i = 0} \]

Write

\[ P = P_h + P' \]

where \( P_h \) homogenous part of deg \( d+1 \)

and \( \deg (P') \leq d \).

Since \( \deg (P_n(x_i)) = d \), we have

that \( P_n(x_i) \) vanishes for every \( x_i \).

In other words, \( x_i \mid P_h \).

But then \( \prod_{i=1}^{d+2} x_i \mid P_h \)

which contradicts \( \deg (P_h) \leq d+1 \).

Lemma 2 follows.

**Lemma 3**

Let \( n \geq k \geq d+1 \) and let \( f : \mathbb{R}^n \to \mathbb{R} \) have

\( \deg (f) > d \). Then \( \text{Reg}_d(k)(f) \geq 2^{k-n} \).

**Proof** Induction on \( n \). Base case \( n = k \) is obvious.

Assume Lemma holds for \( n-1 \).
Pick random hyperplane \( A \subseteq \mathbb{F}_2^n \)

By Lemma 2,

\[
\Pr[ f|A \text{ not degree-}d \text{ polynomial}] \\
\geq \text{ by def} \ \\
\text{Rej}_d, n-1 (f) \\
\geq \frac{1}{2}
\]

Now a random \( k \)-flat in \( A \) will detect that \( f|A \) is not degree-\( d \) with probability \( \geq 2^{k-(n-1)} \).

Claim (iv)

Consider the following two experiments

1. Pick uniformly random \( k \)-flat \( B \) in \( \mathbb{F}_2^n \)
2. Pick uniformly random hyperplane \( C \) in \( \mathbb{F}_2^n \)

Pick uniformly random \( k \)-flat \( C \) in \( C' \).

Then \( B \) and \( C \) have exactly the same distribution.

Using Claim (iv) and above reasoning, we get

\[
\text{Rej}_{d,k} (f) \geq \text{Rej}_{d,n-1} (f) \cdot \text{Rej}_{d,k} (f|A) \\
\geq \frac{1}{2} \cdot 2^{k-(n-1)} \\
= 2^{k-n}
\]

(assuming \( f|A \) is not degree-\( d \) poly) \( \square \)
Proof of Lemma C

For \( k > k' \), we view \( k' \)-flat test as follows:

(a) Pick random \( k \)-flat \( A \subseteq \mathbb{F}_2^k \)
(b) Pick random \( k' \)-flat \( A' \subseteq A \)
(c) Accept if \( fA' \) is degree-\( d \) polynomial

By a generalization of Claim (iv), this is exactly the same as the standard description of the \( k' \)-flat test.

\[ \Pr[fA, \text{ not degree-}d] = \text{Rej}_d(k')(f) \]

by definition. By Lemma 3

\[ \Pr[(f^\star A_1)_{A'}, \text{ not degree-}d] = \text{Rej}_d(k')(f) \cdot 2^{-(k-k')} \]

Hence,

\[ \text{Rej}_d(k')(f) = \Pr[(f^\star A_1)_{A'}, \text{ not degree-}d] \geq \text{Rej}_d(k')(f) \cdot 2^{-(k-k')} \]

and Lemma C follows.

Good, so now we're done with the easy Lemmas A and C. Time to move on to Lemma B!
Proof of Lemma B

Prove Lemma for any
\[ \beta < 1/24 \]
\[ \epsilon_0 < 1/8 \]
\[ \gamma > 72 \]
\[ c \geq \log_2 \left( \max \left\{ \frac{4\gamma}{1-8\epsilon_0} , \frac{5}{1-\epsilon_0} , \frac{2}{\beta \gamma} \right\} \right) \]

In particular, \( \beta = 1/25 \), \( \epsilon_0 = 1/16 \), \( \gamma = 72 \), \( c = 10 \) works.

The proof is by induction over \( (n-k) \).

Want to prove that for \( n \geq k \geq \text{dist} \) that if \( E(f, P, k) \geq \beta \cdot 2^{-\gamma} \) then \( R_{\text{dist}}(f) \geq \epsilon_0 + \gamma \cdot 2^{-k/n} \).

Base case \( n-k = 0 \)

Then \( R_{\text{dist}}(f) = 1 \geq \epsilon_0 + \gamma \cdot 2^{-k} \)

since \( 2^{-k} \leq 2^{-c} \leq \frac{2^{c}}{1-\epsilon_0} \)

Inductive step

Let \( \mathcal{H} \) be the hyperplanes in \( \mathbb{H}^n \setminus \mathbb{P}^n \)

\[ |\mathcal{H}| = N = 2(2^n-1) \quad \text{[by Pop 1.1]} \]

Let \( \mathcal{H}^* \) be the set of all hyperplanes \( A \in \mathcal{H} \) such that

\[ E(f, A, P, k) \leq \beta \cdot 2^{-\gamma} \]

Let \( K = |\mathcal{H}^*| \)
Since a random \( k \)-flat of a random hyperplane is a random \( k \)-flat (Claim (d)), we have

\[
\text{Reg}_{d,k} (f) = \mathbb{E}_{A \in \mathcal{H}} \left[ \text{Reg}_{d,k} (f|A) \right] 
\]

By induction, for \( A \in \mathcal{H} \setminus \mathcal{H}^* \) we have

\[
\text{Reg}_{d,k} (f|A) \geq \epsilon_0 + \gamma \cdot \frac{2^d}{2^{n-1}} 
\]

and hence

\[
\text{Reg}_{d,k} (f) \geq \left( 1 - \frac{K}{N} \right) \cdot \left( \epsilon_0 + \gamma \cdot \frac{2^d}{2^{n-1}} \right) 
\]

\[
\geq \epsilon_0 + \gamma \cdot \frac{2^d}{2^{n-1}} - \frac{K}{N} \tag{3}
\]

We get a case analysis depending on whether \( K = |\mathcal{H}^*| \) is small or large.

**Case 1**: \( K \leq \gamma \cdot 2^d \) \([f \text{ far from degree-}d \text{ poly}]\)

Then massaging (3) further we obtain

\[
(3) \geq \epsilon_0 + \gamma \cdot \frac{2^d}{2^n} \cdot 2 - \gamma \cdot \frac{2^d}{2^{n-1}} 
\]

\[
\geq \epsilon_0 + \gamma \cdot \frac{2^d}{2^n} - \gamma \cdot \frac{2^d}{2^n} 
\]

\[
= \epsilon_0 + \gamma \cdot \frac{2^d}{2^n}
\]
If this happens, for many hyperplanes there are polynomials \( P_\lambda \) such that \( \delta(f, P_\lambda) \leq \text{small} \).

We want to show that these local polynomials \( P_\lambda \) can be sewn together to global polynomial that is close to \( f \) on all of \( \mathbb{F}_2^n \).

**Lemma ("Sewing Lemma")**

For \( f : \mathbb{F}_2^n \to \mathbb{F}_2 \), let \( A_1, ..., A_k \) be hyperplanes such that \( f \mid A_\lambda \) is \( \alpha \)-close to some degree-\( d \) polynomial on \( A_\lambda \). Then if \( K > 2d+1 \) and \( \alpha < 2^{-(d+2)} \), it holds that

\[
\delta(f, P_\lambda) \leq \frac{3}{2} \alpha + \frac{9}{K}
\]

In (3), set \( \alpha = \beta \cdot 2^{-d} < 2^{-(d+2)} \)

Note that \( K > \delta \cdot 2^{d} > 2^{d+1} \)

Hence

\[
\delta(f, P_\lambda) \leq \frac{3}{2} \beta \cdot 2^{-d} + \frac{9}{\delta \cdot 2^{d}} = \delta_0
\]

Since

\[
\beta < 1/24
\]

\[
\frac{9}{\delta} < 1/8
\]

we get \( \delta_0 < \frac{1}{16} 2^{-d} + \frac{1}{8} 2^{-d} < 2^{-d+2} \)
Lemma A now implies that
\[ \text{Rjd, } h(f) = \min \left\{ 2^k + \delta(f, P_k) : \frac{1}{8} \right\} \]

We claim both terms on RHS are
\[ \geq \varepsilon_0 + \frac{y}{2\varepsilon_0} \]
\[ \geq \varepsilon_0 + \frac{y}{2^{d/2^k}} \quad \text{(since } n > k > \text{dic) } \]

By the setting of parameters at start of proof, we have
\[ 2^C \geq \frac{4\xi}{1 - 8\varepsilon_0} \]
\[ 1 - 8\varepsilon_0 \geq \frac{4\xi}{2C} \]
\[ \frac{1}{8} \geq \varepsilon_0 + \frac{y}{2^{d/2^k}} \]

Taking case of the second term. Since also
\[ 2^C \geq 2^{1/\beta} \]
we have \( \beta \geq 2^{c+1} \) and
\[ 2^{k-1} \delta(f, P_k) \geq 2^{k-1} \cdot \beta \cdot 2^{-d} \]
\[ \geq 2^{c-1} \cdot \beta \]
\[ \geq 2^{c-1} \cdot 2^{-c+1} = 1 \]

Hence
\[ \text{Rjd, } h(f) \geq \varepsilon_0 + \frac{y}{2^{d/2^k}} \]
and lemma B follows by the induction principle.
We'll spend what remains of this lecture proving (or at least trying to prove) the Sensing Lemma.

High-level idea:

0. By assumption find hyperplanes $A_1, \ldots, A_K$ such that $f | A_i$ is close to some polynomial $P_{A_i}$ on $A_i$.

0. Use $P_{A_i}$ to define $P \in \mathbb{F}_2[x_1, \ldots, x_n]$ on whole space of degree $\deg(P) = \max_i \deg(P_{A_i}) \leq d$.

0. Show that $P$ agrees with $P_{A_i}$ on $A_i$; hence on every $A_i$, $f$ and $P$ are close.

0. Suppose $A_i$ would cover $\mathbb{F}_2^n$ exactly uniformly:

$$\forall x, z \in \mathbb{F}_2^n \left( \left| \{ A_i | x \in A_i \} \right| = \left| \{ A_j | z \in A_j \} \right| \right)$$

then we would get $\delta(f, P) \leq \varepsilon$ and be done (with some margin).

0. This is a bit too much of wishful thinking, but the coverage is almost uniform so above argument kind of works if we allow for some slack:

$$\delta(f, P) = \frac{3}{2} \varepsilon + \frac{9}{K} \text{ instead of } \delta(f, P) \leq \varepsilon.$$

And the Sensing Lemma follows:

For every $A_i$, fix $P_i$ degree-$d$ polynomial such that $f | A_i$ is $\varepsilon$-close to $P_i$. 
SUBLEMMA 5

Suppose $A_i, A_j$ non-complementary hyperplanes $(A_i \cup A_j \neq \mathbb{F}_2^n)$. Then $P_i \Gamma A_i \cap A_j = P_i \Gamma A_i \cap A_j$ if $x < 2 - (d + 2)$.

$|A_i \cap A_j| = |A_i|/2 = |A_j|/2$

This is so since

$A_i = \{ x \mid \ell_i(x) = 0 \}$

$A_j = \{ x \mid \ell_j(x) = 0 \}$

Since $A_i \neq A_j$, there is non-empty intersection, say $x^*$. Then all points are given by $x^* + y$

where $y$ solution to $\ell_i(y) = 0$

$\ell_j(y) = 0$

$2^{n-2}$ solutions. $|A_i| = |A_j| = 2^{n-1}$

Worst case: all disagreements between $f$ and $P_i \Gamma P_j$ on $A_i \cap A_j$. If so, you have

$\delta(f \setminus A_i \cap A_j, P_i \Gamma A_i \cap A_j) \leq 2x$

$\delta(f \setminus A_i \cap A_j, P_j \Gamma A_i \cap A_j) \leq 2x$

By $\Delta$-inequality

$\delta(P_i \Gamma A_i \cap A_j, P_j \Gamma A_i \cap A_j) \leq 4x < 2 - d$

But 2 degree-$d$ polynomials agreeing in all but 2-$d$ fraction of points are the same. $\Box$
Let $c = \left\lfloor \log_2 (d+1) \right\rfloor$
Then $c > d$

By Prop. 11(2), $d$ linearly independent hyperplanes.
Assume WLOG $A_1, A_2, \ldots, A_c$.

By Prop. 11(3), assume WLOG for $i \in [c]$
$$A_i = \{ x \in \mathbb{F}_2^n \mid x_i = 0 \}$$

Can view $P_i$ as polynomial $P_i \in \mathbb{F}_2[x_1, \ldots, x_n]$ not containing any $x_i$.

Let us write below
$$x = (x_1, \ldots, x_c)
$$
$$y = (x_{c+1}, \ldots, x_n)$$

Can write any $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ as
$$f(x, y) = \sum_{S \subseteq [c]} P_{i_S}(y) \prod_{j \in S} x_j \quad (4)$$

In particular write
$$P_i = P_c(x, y) = \sum_{S \subseteq [c]} P_{i_S}(y) \prod_{j \in S} x_j \quad (5)$$

We have
$$\deg (P_{i_S}) \leq d - |S| \quad (6)$$
$$|S| > d \Rightarrow P_{i_S} = 0 \quad (7)$$

Since $x_i$ doesn't occur in $P_i$; also
$$i \in S \Rightarrow P_{i_S} = 0 \quad (8)$$
and so

\[ P_i(x,y) = \sum_{S \subseteq [t] \setminus \{i,j\}} P_i,s(y) \prod_{j \in S} x_j \]  \hspace{1cm} (9)

**SUBLEMMA 6**

For every \( S \subseteq [t] \), \( i,j \in [t] \setminus S \) it holds that \( P_i,s(y) = P_j,s(y) \)

**Proof:** To evaluate \( P_i,s \) on \( A_j = \{ x \in \mathbb{F}_2^n \mid y = 0 \} \) we simply set \( x_j = 0 \). Hence

\[ P_i \setminus A_j (x,y) = \sum_{S \subseteq [t] \setminus \{i,j\}} P_i,s(y) \prod_{j \in S} x_j \]

\[ P_j \setminus A_i (x,y) = \sum_{S \subseteq [t] \setminus \{i,j\}} P_j,s(y) \prod_{i \in S} x_i \]

**Claim (v)**

Any \( f : \mathbb{F}_2^n \to \mathbb{F}_2 \) has a unique representation as a multilinear polynomial over \( \mathbb{F}_2 [x_1, ..., x_n] \)

By **Sublemma 5**, \( P_i \setminus A_j = P_j \setminus A_i \)

Combining this with **Claim (v)**, these polynomials must be the same syntactically, and hence

\[ P_j,s(y) = P_i,s(y) \]

as claimed \( \Box \)
Hence, we can define for $S \subseteq [l]$

$$P_s(y) = P_{i,y}(y) \quad \text{for any } i \in [l] \setminus S$$

(10)

Now we can define our serving polynomial

$$P(x,y) = \sum_{S \subseteq [l]} P_s(y) \prod_{j \in S} x_j$$

(11)

By (6), (7), and (10) we have $\deg(P) \leq d$.

We want to show that

$$\delta(f, P) \leq \frac{3}{2} \alpha + \frac{9}{K}$$

Let us start by showing that $P$ agrees with any $P_i$ on $A_i$ for $i = 1, \ldots, K$ (not just for $i \subseteq S$)

**Lemma 7**

For every $i \in [K]$, $P_i | A_i = P_i \setminus A_i$.

**Proof.** For $i \in [K]$ we can just plug $x_i = 0$ into expressions (9) and (11) (using also (10)).

Consider $i \in [K] \setminus [l]$.

For any $x \in A_i \cap \bigcup_{j=1}^l A_j$, letting $j^* \in [l]$ be such that $x \in A_{j^*}$ we have

$$P_i(x) = P_{j^*}(x)$$

by Sublemma 5 and also
\[ P_{j^*}(x) = P(x) \]

by what we just showed, since \( j^* \in [L] \)

Hence, \( P_c \) and \( P \) agree on \( A_i \cap U_{j^*}^c A_j \)

Claim (vi)

Since \( c > c \), it holds that

\[ \left| A_i \cap \bigcup_{j=1}^{L} A_j \right| \geq 1 - 2^{-c} > 1 - 2^{-c} \]

Since \( P_{PiA_i} \) are both of degree \( \leq d \), they must be identical. Hence

\( P_{PiA_i} = P_{PiA_i} \) for all \( i \) and the sublemma follows.

Hence \( P \) is close to \( f \) on every hyperplane.

Recall that if \( A_1, \ldots, A_k \) covered all of \( \mathbb{F}_2^n \) uniformly, then we would immediately get

\[ \delta(f, P) \leq \epsilon \]

We'll argue instead that

- most of \( \mathbb{F}_2^n \)
- is covered roughly uniformly

and this will be good enough.

To this end, let

\[ \mathbf{BAD} = \{ z \in \mathbb{F}_2^n \mid \exists \alpha A_i \text{ for less than } K/3 \text{ hyperplanes } A_i \} \]

\[ \epsilon = \frac{|BAD|}{2^n} \]
We have two final sublemmas.

**Lemma 8**

\[ \delta(f, P) \leq \frac{3}{2} \alpha + \varepsilon \]

**Lemma 9**

\[ \varepsilon \leq q/K \]

Combining sublemmas 8 and 9, the Sennig Lemma immediately follows.

**Proof of Lemma 8**

Consider the following experiment:

Pick \( z \in \mathbb{F}_2^n \) and \( i \in K \) uniformly and independently at random.

Let \( E_{z,i} \); \( z \in A_i \) and \( f(z) + P_i(z) \)

What is \( \Pr \left[ E_{z,i} \right] \)?

On the one hand,

\[ \Pr \left[ E_{z,i} \right] \leq \max_i \left\{ \Pr \left[ z \in A_i \right] \cdot \Pr \left[ f(z) + P_i(z) \mid z \in A_i \right] \right\} \]

\[ \leq \frac{1}{2} \cdot \alpha \]

(12)

On the other hand, since \( P_i A_i = P_i \), we can calculate the probability as
\[ \Pr \left[ z \in A_i \right] = \Pr \left[ z \in A_i \right. \text{ and } f(z) \neq P(z) \bigg] \\
\geq \Pr \left[ z \in A_i \right. \text{ and } f(z) \neq P(z) \bigg. \text{ and } z \notin \text{BAD} \bigg] \\
= \Pr \left[ f(z) \neq P(z) \right. \text{ and } z \notin \text{BAD} \bigg] \cdot \Pr \left[ \left. z \in A_i \bigg| f(z) \neq P(z) \right. \text{ and } z \notin \text{BAD} \right] \\
\geq \Pr \left[ f(z) \neq P(z) \right. \text{ and } z \notin \text{BAD} \bigg] \cdot \min_{z: z \notin \text{BAD}} \Pr \left[ \left. z \in A_i \right| f(z) \neq P(z) \right] \\
\geq \left( \delta(f, P) - \varepsilon \right) \cdot \min_{z: z \notin \text{BAD}} \Pr \left[ \left. z \in A_i \right| f(z) \neq P(z) \right] \\
\geq \left( \delta(f, P) - \varepsilon \right) \cdot \frac{1}{3} \\
\text{using } \Pr \left[ A \land \neg B \right] \geq \Pr \left[ A \right] - \Pr \left[ B \right] (13) \\

Combining (12) and (13) we get that \\
\left( \delta(f, P) - \varepsilon \right) / 3 \leq \varepsilon / 2 \\
from which the sublemma follows \square
Proof of Sublemma 9

Let \( x \sim \mathbb{F}_2^n \) uniformly randomly distributed. For \( i \in [K] \), define
\[
Y_i = Y_i(z) = \begin{cases} 
1 & \text{if } z \in A_i \\
-1 & \text{otherwise}
\end{cases}
\]

\( z \in \text{BAD} \) iff \( \sum_{i=1}^{K} Y_i(z) \leq -K/3 \)

Hence
\[
\mathcal{Z} = \mathbb{P}_{\mathbb{F}_2^n} \left[ \sum_{i=1}^{K} Y_i \leq -K/3 \right] \quad (14)
\]

Since \( A_i \) is exactly half of \( \mathbb{F}_2^n \) we have
\[
\mathbb{E}[Y_i] = 0
\]
\[
\text{Var}(Y_i) = \mathbb{E}[Y_i^2] - (\mathbb{E}[Y_i])^2 = 1
\]

Claim (vii)

If \( A_i \) and \( A_j \) are not complementary hyperplanes, then \( Y_i \) and \( Y_j \) are independent and so \( \mathbb{E}[Y_i Y_j] = \mathbb{E}[Y_i] \mathbb{E}[Y_j] = 0 \).

If \( A_i \) and \( A_j \) are complementary, then
\[
\mathbb{E}[Y_i Y_j] = -1 \leq 0
\]
Hence
\[
\mathbb{E}\left[ \sum_{i=1}^{K} Y_i \right] = 0 \quad (15)
\]
\[
\text{Var}\left( \sum_{i=1}^{K} Y_i \right) \leq K \quad (16)
\]
(Recall that)
\[
\text{Var}(\sum_i Y_i) = \sum_i \text{Var}(Y_i) + 2 \sum_{i<j} \text{Cov}(X_i, X_j)
\]

and we have
\[
\text{Cov}(Y_i, Y_j) = E[XY_iY_j] - E[X_i]E[Y_j]
= E[Y_iY_j] - E[Y_i]E[Y_j]
= 0 
\]

**Chebyshev’s Inequality**

If \(X\) is a random variable with
\[\text{Var}(X) = \sigma^2\], then for every \(k > 0\)

it holds that
\[
\Pr\left[\left| X - E[X] \right| > k \sigma \right] \leq \frac{1}{k^2}
\]

Using Chebyshev's inequality, we get
\[
\mathcal{V} = \Pr\left[ \sum_i Y_i \leq -K/3 \right]
\leq \Pr\left[ \left| \sum_i Y_i - E[\sum_i Y_i] \right| \geq K/3 \right]
\leq \text{Var}(\sum_i Y_i) \quad \text{(since \( k \cdot \sqrt{\text{Var}(\sum_i Y_i)} = K/3 \))}
\leq \frac{\text{Var}(\sum_i Y_i)}{(K/3)^2}
\leq \frac{9 \cdot K}{K^2} = \frac{9}{K}
\]

This establishes the second lemma, and hence Lemma B, in [BKSSZ10].