SECTION 5. THE FUNDAMENTAL LEMMA.

We will work in the integers. The coefficients of polynomials, and all variables will be integers.

Notation: We will consider a polynomial $P(X) = a_0X^n + a_1X^{n-1} + \ldots + a_n = \sum_{p=0}^{n} a_p X^{n-p}$, integers m and N, with $N \geq 1$. For an arbitrary integer $g \geq 1$, recall that $r_{PNg}(m)$ is the number of g-tuples $(x_1, x_2, \ldots, x_g)$ such that for $1 \leq i \leq g$, we have $|x_i| \leq N$ and also $P(x_1) + P(x_2) + \ldots + P(x_g) = m$.

Notation: Let $k(2) = 3$ and for $n > 2$, let $k(n) = n$.
Let $g(1) = 2$, and for $n \geq 2$, let $g(n) = k(n)2^{\lceil(\log_2 g(n-1))+2\rceil}$.
Also, let $F(1) = 0$ and for $n \geq 2$, let $F(n) = k(n)(F(n-1) + 1)$.

Notation: In what follows, for $n \geq 2$ we will let k denote k(n), and g denote g(n). Also, we will let $q = g/2$, $g' = g(n-1)$, and $s = \lceil(\log_2 g') + 2\rceil - 1$. (Thus $g = 2^{s+1}k$ and $q = 2^s k$.)

Heuristic comment: We will use lemma 6, which discusses a number of the form $q = 2^s k$. That explains the need for the basic form of g(n). A later heuristic comment will show why s is best taken to be $\lceil(\log_2 g') + 2\rceil - 1$. (Any larger s would also work.) Concerning the definition of k(n), we will later need to have $k(n-1) \leq n(k-1)$. That requires having $k(n) = k \geq n$, and we will have $k(n-1) = n(n-1) = n(k-1)$ when $n > 2$. However, we will also use lemma 9, which requires $k \geq 3$, and so we take k(2) to be 3, not 2. Thus, our k(n) is the least possible. (Any larger k would also work.) Our definition of g(n) seems to be the smallest possible using Linnick's proof of proposition 10. We do not claim it is the smallest making that proposition true.

Notation: For $N \geq 1$, let $C_{PN} = \max\{\frac{|a_p|}{N^p} \mid 0 \leq p \leq n\}$ (which is at least $|a_0| \geq 1$).

Also, let $M_P = \max\{|a_p| \mid 0 \leq p \leq n\}$. (Clearly $M_P \geq C_{PN}$ for any $N \geq 1$.)

Proposition 10: For $n \geq 1$, there is a function $K(n)$ (depending only on n), such that the following is true. If $P(X) = \sum_{p=0}^{n} a_p X^{n-p}$ is a degree $n > 0$ polynomial, and if $N \geq 1$, then for any integer m, we have $r_{PNg}(m) \leq K(n)(C_{PN})^{F(n)}N^{g-n}$ (with $g = g(n)$).

Heuristic comment: It is not difficult to show that for any g, $r_{PNg}(m)$ is at most a constant times N^{g-1}. That is done by selecting $x_2, \ldots, x_g$ arbitrarily (between $-N$ and N), and then noting that at most n choices of x_1 satisfy $P(x_1) + P(x_2) + \ldots + P(x_g) = m$. The exponent $g - 1$ is too big. Our goal is to show that for $g = g(n)$, it can be replaced with $g - n$, as in proposition 10. Furthermore, it is not too hard to see that proposition 10 holds for all $g \geq g(n)$.

Heuristic comment. We here give an insightful 'rough estimate' argument. The triangle inequality shows for any integer x, $|P(x)| \leq \max\{(n + 1)M_P|x|^n, |a_0|\}$ (the appearance of a_0 needed when $x = 0$). If $|x| \leq N$ and $|a_0| \leq N$, then $|P(x)| \leq (n + 1)M_PN^n$. Therefore, if $(x_1, x_2, \ldots, x_g)$ is such that for $1 \leq i \leq g$, we have $|x_i| \leq N$ and also $P(x_1) + P(x_2) + \ldots + P(x_g) = m$, then $|m| \leq (g)(n + 1)M_PN^n$.

As a rough estimate, there are about $2(g)(n + 1)M_PN^n$ choices for m satisfying that inequality. On the other hand, a rough estimate of the number of $(x_1, x_2, \ldots, x_g)$ with all $|x_i| \leq N$ is about $(2N)^g$. Taking an average, we would 'expect the average m' to have $m = P(x_1) + P(x_2) + \ldots + P(x_g)$ be true for about $\frac{(2N)^g}{2(g)(n+1)M_PN^n} = \frac{2^{g-1}}{(g)(n+1)M_P}N^{g-n}$

choices of $(x_1, \ldots, x_g)$. Now in fact the coefficient $K(n)(C_{PN})^{F(n)}$ in proposition 10 will be larger than $\frac{2^{g-1}}{(g)(n+1)M_P}$. That allows the possibility that some m might possibly use up more than their fair share of the $(x_1, \ldots, x_g)$. But the main import of proposition 10 is that it shows no m uses too many more than its fair share of the $(x_1, .., x_g)$. That means many choices of m have a decent shot at being expressed in the form $m = P(x_1) + P(x_2) + \ldots + P(x_g)$. That fact is essentially the heart of Linnick's argument.

We now use proposition 10 to prove the fundamental lemma used in section 2. (The K mentioned there is the $K(n)(M_P)^{F(n)}$ mentioned here.)

Fundamental lemma: For any degree n polynomial P(X), any $N \geq 1$, and any integer m, $r_{PNg}(m) \leq K(n)(M_P)^{F(n)}N^{g-n}$. Furthermore, for N sufficiently large, $r_{PNg}(m) \leq K(n)|a_0|^{F(n)}N^{g-n}$.

Proof: The first statement follows from the Proposition 10 and the fact that $M_P \geq C_{PN}$. As for the second statement, $\frac{|a_p|}{N^p}$ is just $|a_0|$ when p = 0. However, for $2 \leq p \leq n$, that fraction goes to 0 as N goes to infinity. Therefore, for large enough N, $C_{PN} = |a_0|$, and the second statement follows from Proposition 10.

Heuristic comment: We will use induction on n to prove proposition 10. A subtlety is that the fundamental lemma cannot be proved directly via induction. This will be explained more fully at the end.

Heuristic comment: In the expression $K(n)(C_{PN})^{F(n)}N^{g-n}$, it is the exponent $g - n$ which is important. The constant $K(n)(C_{PN})^{F(n)}$ is of little importance, except that it exists and depends only on n and P(X). In section 2, we simply used K to denote $K(n)(C_{PN})^{F(n)}$. However, at the risk of being overly pedantic, we chose to here parse that K, finding which part of it depends only on n, and which part depends on the polynomial itself. The two resulting parts are the K(n) and the $(C_{PN})^{F(n)}$. We did give a formula for F(n) since it is easy to find, not because it is important.

Notational comment: We recursively defined $g(n)$ and $F(n)$. Similarly, $K(n)$ is defined recursively, starting with $K(1) = 3$, as we will soon see. However, we will not make the definition of $K(n)$ explicit, since it is a bit elaborate. Instead, we will leave a trail of symbols K_i, for $1 \le i \le 11$. Each K_i will be a function solely of n. We will eventually see that $K(n) = K_1K_3K_9$. The sufficiently masochistic reader is free to use our trail to find the actual definition of $K(n)$. (We do not claim it is the smallest possible.)

Note that g, g′, q, k and s are all solely functions of n, and so our various K_i can depend upon any of them. Sometimes, we will let the reader figure out the definition of some K_i. For example, $(K_iN)^q$ might simply be written as K_jN^q, without saying that $K_j = K_i^q$.

We do mention that $K(n-1)$ will be incorporated into K_{11}, from whence $(K(n-1))^k$ ends up as a factor of $K(n)$.

We now turn to the proof of proposition 10. The proof is by induction on the degree n of $P(X)$. For the case $n = 1$, we have $g(1) = 2$. We are considering (x_1, x_2) with $|x_i| \le N$ and with $P(x_1) + P(x_2) = m$. Since $-N \le x_2 \le N$, x_2 can be chosen in at most $2N + 1 \le 3N$ ways. Since the degree of $P(X)$ is 1, for each x_2, there are at most one choice for x_1 with $P(x_1) + P(x_2) = m$. Therefore, with $K(1) = 3$, and $F(1) = 0$, we have $r_{PN2}(m) \le 3N = K(1)(C_{PN})^{F(1)}N^{2-1}$, as required.

We now suppose proposition 10 holds for $n - 1 \ge 1$. Fixing $N \ge 1$ and an integer m, we wish to bound $r_{PNg}(m)$, the number of $(x_1, x_2, \ldots x_q, x_{q+1}, \ldots, x_g)$ with each $|x_i| \le N$, and with $P(x_1) + P(x_2) + \ldots + P(x_q) + P(x_{q+1}) + \ldots + P(x_g) = m$. Letting A be the complex of numbers of the form $P(x_1) + P(x_2) + \ldots + P(x_q)$ with $|x_i| \le N$, we see that $r_{PNg}(m)$ is the M-number of (a_1, a_2) with both components in A, and satisfying $a_1 + a_2 = m$. (The multiplicities in A arise from the fact that different choices of $(x_1, \ldots, x_q)$ might give equal values to $P(x_1) + P(x_2) + \ldots + P(x_q)$.) Corollary 7 tells us $r_{PNg}(m)$ is at most the M-number of solutions of $a - a' = 0$ with a and a′ in A. We call that M-number r_{PNg}, and note that it can also be described as the number of $(x_1, x_2, \ldots, x_q, y_1, y_2, \ldots, y_q)$ such that each $|x_i|$ and $|y_i|$ is at most N, and such that $(P(x_1) + \ldots + P(x_q)) - ((Py_1) + \ldots + P(y_q)) = 0$.

The previous paragraph shows $r_{PNg}(m) \le r_{PNg}$, and so it will suffice to prove that $r_{PNg} \le K(n)(C_P)^{F(n)}N^{g-n}$. (This shows why the bound $K(n)(C_P)^{F(n)}N^{g-n}$ is independent of m.)

Given $(x_1, x_2, \ldots, x_q, y_1, y_2, \ldots, y_q)$ as above, let $h_t = x_t - y_t$ for $1 \le t \le q$. Obviously r_{PNg} equals the number of $(h_1, h_2, \ldots, h_q, y_1, y_2, \ldots, y_q)$ with $|y_t + h_t|$ and $|y_t|$ both at most N, and with $(P(y_1 + h_1) + \ldots + P(y_q + h_q)) - ((Py_1) + \ldots + P(y_q)) = 0$. We see that we must have $|h_t| \le 2N$, and so clearly $r_{PNg} \le R_{PNg}$, the latter denoting the number of $(h_1, h_2, \ldots, h_q, y_1, y_2, \ldots, y_q)$ with $|h_t|$ and $|y_t|$ both at most 2N, and with $0 = (P(y_1 + h_1) + \ldots + P(y_q + h_q)) - ((Py_1) + \ldots + P(y_q))$ $= \sum_{t=1}^{q}(P(y_t + h_t) - P(yt))$. Obviously, it will suffice to show $R_{PNg} \le K(n)(C_P)^{F(n)}N^{g-n}$.

Let us fix a q-tuple $H = (h_1, .., h_q)$ with each $|h_t| \le 2N$, and let R_{HPNg} be the number of $(y_1, \ldots, y_q)$ such that $|y_t| \le 2N$ and $(H, y_1, \ldots, y_q) = (h_1, h_2, \ldots, h_q, y_1, y_2, \ldots, y_q)$ is a solution of $\sum_{t=1}^{q}(P(y_t + h_t) - P(y_t)) = 0$. Note that $R_{PNg} = \sum_{H} R_{HPNg}$, the sum over all allowable q-tuples H.

We leave to the reader the exercise of using the binomial theorem to show

$P(y + h) - P(v) = h\Phi(h, y)$ with $\Phi(h, y) = \sum_{u=0}^{n-1} b_u(h) y^{(n-1)-u}$, where $b_u(h) = \sum_{p=0}^{u} a_p \binom{n-p}{u+1-p} h^{u-p}$.

We see that R_{HPNg} is the number of $(y_1, \ldots, y_q)$ such that $|y_t| \le 2N$ and $(H, y_1, \ldots, y_q)$ is a solution of $\sum_{t=1}^{q} h_t \Phi(h_t, y_t) = 0$.

Heuristic comment: $\Phi(h, y)$ has degree $n - 1$ in the variable y. That will eventually let us do our induction. However, in the equation above, the polynomial $\Phi(h_t, y)$ varies with h_t. Thus, we actually have q different polynomials of degree $n - 1$, one for each h_t. That is bad. We will use lemma 6 to convert the situation into one in which we only have k different versions of Φ, each one appearing 2^s times. That is good, as we will later see.

In section 3, we considered complexes named by subscripted letters A. Here, we will use subscripted A(H), to reflect that our choice of $H = (h_1, .., h_q)$ plays a role in the definition of our complexes. Specifically, for $1 \le t \le q$, let $A(H)_t$ be the complex of numbers of the form $X_t = P(y_t + h_t) – P(y_t) = h_t\Phi(h_t, y_t)$, with $|y_t| \le 2N$. (Obviously multiplicities are involved since two different choices for y_t might lead to the same X_t.) Each one of the $(y_1, \ldots, y_q)$ we are counting to find R_{HPNg} gives an $(H, y_1, y_2, \ldots, y_q)$, which in turn gives a $(X_1, \ldots, X_q)$ forming a solution of

(%) $X_1 + X_2 + \ldots + X_q = 0$ with $X_t \in A(H)_t$.

Conversely, each solution $(X_1, \ldots, X_q)$ of (%) arises from one or more such $(y_1, \ldots, y_q)$. Therefore, R_{HPNg} equals the M-number of solutions $(X_1, \ldots, X_q)$ of (%).

We now convert indices to the notation of section 3. Recall that $q = g/2 = 2^s k$. We will let w vary from 0 to $2^s – 1$, while i varies from 1 to k. Thus $\{wk + i \mid 0 \le w \le 2^s - 1, 1 \le i \le k\} = \{1, 2, \ldots, q\}$. The index t used in the previous paragraph will be replaced by wk + i.

Under that change of indices, $(X_1, \ldots, X_q)$ becomes

$(X_1, \ldots, X_k, X_{k+1}, \ldots, X_{k+k}, \ldots, X_{wk+1}, \ldots, X_{wk+k}, \ldots X_{(2^s-1)k+1}, \ldots, X_{(2^s-1)k+k})$,

and (%) becomes

(%%) $\sum_{w=0}^{2^s-1} \sum_{i=1}^{k} X_{wk+i} = 0$, with $X_{wk+i} \in A(H)_{wk+i}$.

We already know that R_{HPNg} equals the M-number of such q-tuples satisfying (%%).

By Lemma 6, $R_{HPNg} \le \frac{1}{2^s}\sum_{w=0}^{2^s-1} M\#\,A(H)skw$. Therefore, $R_{PNg} = \sum_{H} R_{HPNg} \le \frac{1}{2^s}\sum_{H} \sum_{w=0}^{2^s-1} M\#\,A(H)skw = \frac{1}{2^s}\sum_{w=0}^{2^s-1}\sum_{H} M\#\,A(H)skw$. Since we want $R_{PNg} \le K(n)(C_P)^{F(n)}N^{g-n}$, it will suffice to show $\frac{1}{2^s}\sum_{w=0}^{2^s-1}\sum_{H} M\# A(H)skw \leq K(n)(C_P)^{F(n)}N^{g-n}$.

To most easily understand what follows, we will think of our q-tuple H as a concatenation of 2^s sub-k-tuples, $H = (H_0, \ldots, H_w, \ldots, H_{2^s-1})$, with $H_w = (h_{wk+1}, .., h_{wk+k})$.

Let us consider some M#A(H)skw, for a fixed w. By definition (section 3), that number equals the M-number of q-tuples $(a_{j,wk+i} \mid 1 \leq j \leq 2^s, 1 \leq i \leq k)$ such that $a_{j,wk+i} \in A(H)_{wk+i}$, and which give a solution of

$$0 = (a_{1,wk+1} + ... + a_{1,wk+k}) + \ldots + (a_{2^{s-1},wk+1} + ... + a_{2^{s-1},wk+k})$$
$$- (a_{2^{s-1}+1,wk+1} + ... + a_{2^{s-1}+1,wk+k}) - \ldots - (a_{2^s,wk+1} + ... + a_{2^s,wk+k}).$$

Since $a_{j,wk+i}$ is in $A(H)_{wk+i}$, it has the form $h_{wk+i}\Phi(h_{wk+i}, y_{wk+i})$, with $|y_{wk+i}| \leq 2N$. Since $H = (H_0, \ldots, H_w, \ldots, H_{2^s-1})$, we see that in calculating M#A(H)skw, the only part of H which concerns us is the sub-k-tuple H_w, since that is the part of H from whence come the h_{wk+i} we need. Therefore, if $H' = (H_0', \ldots, H_w', \ldots, H_{2^s-1}')$, then M#A(H)skw will equal M#A(H′)skw so long as $H_w = H_w'$. (We do not claim the converse.)

Consider a k-tuple $\overline{H} = (h_1, \ldots, h_k)$ with each $|h_i| \leq 2N$. For a given $H = (H_0, \ldots, H_w, \ldots, H_{2^s-1})$, we will write $H \equiv_w \overline{H}$ to mean $H_w = \overline{H}$. In view of the conclusion of the previous paragraph, we can define M#A($\overline{H}$)sk to be M#A(H)skw for any q-tuple H satisfying $H \equiv_w \overline{H}$. We thus see that $\sum_{H} M\# A(H)skw = \sum_{\overline{H}}\sum_{H\equiv_w \overline{H}} M\# A(\overline{H})sk$, the outer sum over all allowable k-tuples $\overline{H}$.

Obviously $\sum_{H\equiv_w \overline{H}} M\# A(\overline{H})sk = |\{H \mid H \equiv_w \overline{H}\}|$M#A($\overline{H}$)sk. We now bound the size of the set $\{H \mid H \equiv_w \overline{H}\}$. If we build an $H = (H_0, \ldots, H_w, \ldots, H_{2^s-1})$ using $\overline{H}$ for H_w, that leaves q – k other coordinates of H to specify. Each of them lies between -2N and 2N, and so can be chosen in at most 4N + 1 ≤ 5N ways. Therefore, $|\{H \mid H \equiv_w \overline{H}\}| \leq (5N)^{q-k} = K_1N^{q-k}$ (with $K_1 = 5^{q-k}$ being the first of the K_i we discussed earlier.) It follows that

$\sum_{H \equiv_w \overline{H}} M\# A(\overline{H})sk \le K_1N^{q-k}M\#A(\overline{H})sk$, and so from above, we have

$$\sum_{H} M\# A(H)skw = \sum_{\overline{H}} \sum_{H \equiv_w \overline{H}} M\# A(\overline{H})sk \le K_1N^{q-k} \sum_{\overline{H}} M\# A(\overline{H})sk.$$

The right hand side of the above inequality is independent of w. (In building $H = (H_0, \dots, H_w, \dots, H_{2^s-1})$, a random $\overline{H}$ can be used for a random H_w. Our discussion is symmetric in the w.) Therefore, $\sum_{w=0}^{2^s-1} \sum_{H} M\# A(H)skw \le K_1N^{q-k} \sum_{w=0}^{2^s-1} \sum_{\overline{H}} M\# A(\overline{H})sk$

$= 2^sK_1N^{q-k} \sum_{\overline{H}} M\# A(\overline{H})sk$.

Recall that we want to show $\frac{1}{2^s} \sum_{w=0}^{2^s-1} \sum_{H} M\# A(H)skw \le K(n)(C_P)^{F(n)}N^{g-n}$. In view of the preceding, it will suffice to show $K_1N^{q-k} \sum_{\overline{H}} M\# A(\overline{H})sk \le K(n)(C_P)^{F(n)}N^{g-n}$. Dividing by K_1N^{q-k}, we see that we need only show $\sum_{\overline{H}} M\# A(\overline{H})sk \le K_1^{-1}K(n)(C_{PN})^{F(n)}N^{(g-n)-(q-k)}$.

Recall that if n > 2, then k = k(n) = n. In that case, (g – n) – (q – k) = g – q = q. However, if n = 2, then k = k(2) = 3 = n + 1, and so (g – n) – (q – k) = q + 1.

Letting q′ = q + 1 if n = 2, and q′ = q if n > 2, we want to show that

$\sum_{\overline{H}} M\# A(\overline{H})sk \le K_1^{-1}K(n)(C_{PN})^{F(n)}N^{q'}$.

We have not yet defined K(n). Eventually, we will do so in such a way that the above inequality holds for any choice of N ≥ 1.

SECTION 6: ANOTHER REDUCTION.

We recall exactly what $M\#A(\overline{H})sk$ means. We have $\overline{H} = (h_1, \ldots, h_k)$ with each $|h_i| \leq 2N$. The reader can verify that $M\#A(\overline{H})sk$ is the M-number of q-tuples $(a_{j,i} \mid 1 \leq j \leq 2^s, 1 \leq i \leq k)$ giving a solution of

$$(\#)\ 0 = (a_{1,1} + \ldots + a_{1,i} + \ldots + a_{1,k}) + \ldots + (a_{2^{s-1},1} + \ldots + a_{2^{s-1},i} + \ldots + a_{2^{s-1},k})$$
$$- (a_{2^{s-1}+1,1} + \ldots + a_{2^{s-1}+1,i} + \ldots + a_{2^{s-1}+1,k}) - \ldots - (a_{2^s,1} + \ldots + a_{2^s,i} + \ldots + a_{2^s,k}),$$

where each $a_{j,i}$ has the form $h_i\Phi(h_i, v_{j,i})$ with $|v_{j,i}| \leq 2N$.

In (#), the $a_{j,i}$ are grouped together according to the first subscript j. If we regroup, according to the second subscript i, we get

$$(\#\#)\ 0 = (a_{1,1} + \ldots + a_{2^{s-1},1} - a_{2^{s-1}+1,1} - \ldots - a_{2^s,1})$$
$$+ \ldots$$
$$+ (a_{1,i} + \ldots + a_{2^{s-1},i} - a_{2^{s-1}+1,i} - \ldots - a_{2^s,i})$$
$$+ \ldots.$$
$$+ (a_{1,k} + \ldots + a_{2^{s-1},k} - a_{2^{s-1}+1,k} - \ldots - a_{2^s,k}).$$

Substituting $h_i\Phi(h_i, v_{j,i})$ for $a_{j,i}$, we see that $M\#A(\overline{H})sk$ is the number of q-tuples $V = (v_{j,i} \mid 1 \leq j \leq 2^s, 1 \leq i \leq k)$ where each $v_{j,i}$ has $|v_{j,i}| \leq 2N$, and V gives a solution of

$$(\#\#\#)\ 0 = h_1\big(\Phi(h_1,v_{1,1}) + \ldots + \Phi(h_1,v_{2^{s-1},1}) - \Phi(h_1,v_{2^{s-1}+1,1}) - \ldots - \Phi(h_1,v_{2^s,1})\big)$$
$$+ \ldots..$$
$$+ h_i\big(\Phi(h_i,v_{1,i}) + \ldots + \Phi(h_i,v_{2^{s-1},i}) - \Phi(h_i,v_{2^{s-1}+1,i}) - \ldots - \Phi(h_i,v_{2^s,i})\big)$$
$$+ \ldots.$$
$$+ h_k\big(\Phi(h_k,v_{1,k}) + \ldots + \Phi(h_k,v_{2^{s-1},k}) - \Phi(h_k,v_{2^{s-1}+1,k}) - \ldots - \Phi(h_k,v_{2^s,k})\big).$$

Heuristic comment: As promised, we now have k versions of Φ, $\Phi(h_1, v)$ through $\Phi(h_k, v)$, each one appearing with 2^s different choices for v. That will allow us to do our induction, as we will later see. It was the use of lemma 6 which got us to this point. We could have used lemma 6 to get $2^t k$ versions of Φ, each appearing 2^{s-t} times, for any t with $0 \le t \le s$. However, we will see that for our induction, we need to have $g' \le 2^{s-t-1}$. For that, only t = 0 works. A later comment will show that we choose s to be least with $g' \le 2^{s-1}$.

For $1 \le i \le k$, let C_{h_i} be the complex of numbers of the form

$Z_i = \Phi(h_i, v_{1,i}) + \ldots + \Phi(h_i, v_{2^{s-1},i}) - \Phi(h_i, v_{2^{s-1}+1,i}) - \ldots - \Phi(h_i, v_{2^s,i})$ with each $|v_{j,i}| \le 2N$.

Rewriting (###), we get

(####) $0 = h_1Z_1 + \ldots + h_iZ_i + \ldots + h_kZ_k$, with $Z_i \in C_{h_i}$.

Each of our above q-tuples V gives rise to a $(Z_1, \ldots, Z_k)$, and each such k-tuple comes from one or more of the V. Therefore, $M\#A(\overline{H})sk$ (which equals the number of V) equals the M-number of $(Z_1, \ldots, Z_k)$ satisfying (####).

Letting $\overline{H} = (h_1, \ldots h_k)$ vary over all possibilities, we see that $\sum_{\overline{H}} M\# A(\overline{H})sk$ is the M-number of elements in the set T′ =

$\{(h_1, \ldots, h_k, Z_1, \ldots, Z_k) \mid |h_i| \le 2N,\ Z_i \in C_{h_i}$ and satisfying $0 = h_1Z_1 + \ldots + h_iZ_i + \ldots + h_kZ_k\}$.

(The multiplicities of elements in T′ arise from the multiplicities of the Z_i in C_{h_i}.)

Notation: Let us use M#T′ to denote the M-number of elements in T′.

We have just seen that $M\#T' = \sum_{\overline{H}} M\# A(\overline{H})sk$. Therefore, in view of the conclusion of the previous section, we see that it will suffice to show $M\#T' \le K_1^{-1}K(n)(C_{PN})^{F(n)}N^{q'}$.

SECTION 7: THE INDUCTIVE STEP.

As seen at the end of the previous section, we need to bound M#T′. We will first bound it by a constant times |T′|, the constant accounting for the multiplicities. In order to do that, we state a claim whose proof we delay until the end.

CLAIM A: There is a constant K_2 (depending only on n) such that the multiplicity of $Z_i \in C_{h_i}$ is at most $K_2(C_{PN})^{F(n-1)}N^{2^s-n+1}$.

Claim A shows that the multiplicity of any $(h_1, \ldots, h_k, Z_1, \ldots, Z_k)$ in T′, is at most $K_3(C_{PN})^{kF(n-1)}N^{(2^s-n+1)k}$. It follows that $M\#T' \le |T'|K_3(C_{PN})^{kF(n-1)}N^{(2^s-n+1)k}$. The final sentence of section 6 now tells us it will suffice to show $|T'|K_3(C_{PN})^{kF(n-1)}N^{(2^s-n+1)k} \le K_1^{-1}K(n)(C_{PN})^{F(n)}N^{q'}$.

Considering the exponents on both appearances of N in that inequality, we have that $q' - (2^s - n + 1)k = q' - 2^s k + k(n-1) = q' - q + k(n-1)$. Considering the exponents on both appearances of C_{PN}, we have $F(n) - k(F(n-1) = k$, (using that $F(n) = k(F(n-1)+1)$). Therefore, with $K_4 = (K_1K_3)^{-1}$, the previous inequality is equivalent to $|T'| \le K_4K(n)(C_{PN})^kN^{q'-q+k(n-1)}$, and it will suffice to show that.

Recalling the definitions of q′ and k = k(n), we see that if n > 2, then $q' - q + k(n-1) = 0 + n(n-1) = n(n-1)$. However, if n = 2, then $q' - q + k(n-1) = 1 + 3(1) = 4$. Therefore, if n > 2, we want to show $|T'| \le K_4K(n)(C_{PN})^kN^{n(n-1)}$, but if n = 2, we want to show $|T'| \le K_4K(n)(C_{PN})^kN^4$.

Recall that $\Phi(h, y) = \sum_{u=0}^{n-1} b_u(h) y^{(n-1)-u}$, where $b_u(h) = \sum_{p=0}^{u} a_p \binom{n-p}{u+1-p} h^{u-p}$.

Claim B: Suppose $|h| \le 2N$ and $|y| \le 2N$. Then $|b_u(h)| \le 2^{2n-1} C_{PN} N^u$. Also, $|\Phi(h, y)| \le K_5 C_{PN} N^{n-1}$, with $K_5 = 2^{2n-1}(2^n - 1)$ Finally, for any $Z_i \in C_{h_i}$, $|Z_i| \le K_6 C_{PN} N^{n-1}$, with $K_6 = 2^s K_5$.

Proof: The definition of C_{PN} (section 5) shows that for $0 \le p \le n$, we have $|a_p| \le C_{PN} N^p$. Also, we have $u - p \le u \le n - 1$. Therefore,

$$|b_u(h)| \le \sum_{p=0}^{u} |a_p| \binom{n-p}{u+1-p} |h|^{u-p} \le \sum_{p=0}^{u} C_{PN} N^p \binom{n-p}{u+1-p} 2^{u-p} N^{u-p}$$

$\le \sum_{p=0}^{u} C_{PN} N^p \binom{n-p}{u+1-p} 2^{n-1} N^{u-p} = 2^{n-1} C_{PN} N^u \sum_{p=0}^{u} \binom{n-p}{u+1-p}$. Now each term of $\sum_{p=0}^{u} \binom{n-p}{u+1-p}$ is equal to or less than the corresponding term in $\sum_{p=0}^{u} \binom{n}{u+1-p}$. That summation is part of the binomial expansion of $(1 + 1)^n = 2^n$. That shows $|b_u(h)| \le 2^{2n-1} C_{PN} N^u$, proving the first part of the conclusion.

Now $|\Phi(h, y)| \le \sum_{u=0}^{n-1} |b_u(h)| |y|^{n-1-u} \le \sum_{u=0}^{n-1} 2^{2n-1} C_{PN} N^u |y|^{n-1-u} \le \sum_{u=0}^{n-1} 2^{2n-1} C_{PN} N^u (2N)^{n-1-u} =$ $\sum_{u=0}^{n-1} 2^{3n-2-u} C_{PN} N^{n-1} = C_{PN} N^{n-1} \sum_{u=0}^{n-1} 2^{3n-2-u}$. Since $\sum_{u=0}^{n-1} 2^{3n-2-u} = 2^{3n-2} \sum_{u=0}^{n-1} 2^{-u} = 2^{3n-2}\left(\frac{2^n - 1}{2^{n-1}}\right) =$ $2^{2n-1}(2^n - 1)$, the second part of the claim is true.

Finally, any $Z_i \in C_{h_i}$ is the sum/difference of 2^s terms of the form $\Phi(h_i, y)$ with $|h_i| \le 2N$ and $|y| \le 2N$. Therefore, $|Z_i| \le \sum_{j=1}^{2^s} K_2 C_{PN} N^{n-1} = K_6 C_{PN} N^{n-1}$.

The definition of T' (section 6), together with the third conclusion of claim B, makes it clear that T' is a subset of the set

$T'' = \{(h_1, \ldots, h_k, Z_1, \ldots, Z_k) \mid |h_i| \le 2N, |Z_i| \le K_6 C_{PN} N^{n-1}$, and satisfying $0 = h_1 Z_1 + \ldots + h_i Z_i + \ldots + h_k Z_k\}$. Therefore, it will suffice to show $|T''| \le K_4 K(n)(C_{PN})^k N^{n(n-1)}$ if $n > 2$, and $|T''| \le K_4 K(n)(C_{PN})^k N^4$ when $n = 2$.

Heuristic remark: Notice that at this point, all vestiges of $P(X)$ have vanished except its degree n and C_{PN}.

We invoke Lemma 9, letting $F = 2N$ and $D = K_6 C_{PN} N^{n-1}$ (recalling claim B). It tells us that the number of $(h_1, \ldots, h_k, Z_1, \ldots, Z_k)$ in T'' for which at least one h_i is not zero does not exceed $K_7(DF)^{k-1} = K_8(C_{PN})^{k-1} N^{n(k-1)} \le K_8(C_{PN})^k N^{n(k-1)}$, using $C_{PN} \ge 1$.

It remains to bound the number of $(h_1, \ldots, h_k, Z_1, \ldots, Z_k)$ in T'' for which all the h_i are 0. That number clearly equals the number of $(Z_1, \ldots, Z_k)$ with each Z_i in the interval $[-K_6 C_{PN} N^{n-1}, K_6 C_{PN} N^{n-1}]$. Each Z_i can be chosen at most $2K_6 C_{PN} N^{n-1} + 1 \le 3K_6 C_{PN} N^{n-1}$ ways. (Here we used that $C_{PN} \ge 1$. If C_{PN} had been too tiny, that last inequality might not hold.) Therefore, we see that the number of $(h_1, \ldots, h_k, Z_1, \ldots, Z_k)$ in T'' for which all the h_i are 0 is at most $(3K_6)^k (C_{PN})^k N^{k(n-1)}$.

Combining the conclusions of the previous two paragraphs, we see that $|T''| \le K_8(C_{PN})^k N^{n(k-1)} + (3K_6)^k (C_{PN})^k N^{k(n-1)}$.

Suppose $n > 2$. Then $k = n$, so that $k(n-1) = n(k-1) = n(n-1)$. Thus $|T''| \le K_9(C_{PN})^k N^{n(n-1)}$.

Suppose $n = 2$. Then $k = 3$, and $|T''| \le K_8(C_{PN})^k N^4 + (3K_6)^k (C_{PN})^k N^3 \le K_8(C_{PN})^k N^4 + (3K_6)^k (C_{PN})^k N^4 = K_9(C_{PN})^k N^4$.

In either case, we are done, so long as $K_9 \le K_4 K(n)$. We therefore simply define $K(n)$ to be $K_4^{-1} K_9 = k_1 k_3 K_9$.

Heuristic comment: If we had defined k(2) to be 2, we would have gotten that

$|T''| \le CN^2 \sum_{d=1}^{2N} (\frac{1}{d}) \le CN^2(1 + Ln(2N))$ for some constant C. The factor 1 + Ln(2N) is unacceptable to us, since we would have required a bound of the form CN^2.

We have completed the proof of the Fundamental lemma, modulo the proof of Claim B, to which we now turn. It is here that we use our inductive step.

Heuristic comment: The proof of Claim B will require that we have $2^{s-1} \ge g(n-1) = g'$. Thus, we need $s - 1 \ge \log_2 g'$ or equivalently, $s + 1 \ge \log_2 g' + 2$. We also want s + 1 to be an integer, since g(n) must be an integer. Therefore, in the definition of g(n), we took $s + 1 = \lceil (\log_2 g') + 2 \rceil$.

Proof of Claim B: Consider some Z_i in C_{h_i}. We have

$Z_i = \Phi(h_i, v_{1,i}) + \ldots + \Phi(h_i, v_{2^{s-1},i}) - \Phi(h_i, v_{2^{s-1}+1,i}) - \ldots - \Phi(h_i, v_{2^s,i})$, with $|v_{j,i}| \le 2N$.

To simplify notation, let $Q(v) = \Phi(h_i, v)$, and then drop the subscript i from Z_i and from $v_{j,i}$. That is, we are considering the multiplicity of

$Z = Q(v_1) + \ldots + Q(v_{g'}) + \ldots + Q(v_{2^{s-1}}) - Q(v_{2^{s-1}+1}) - \ldots - Q(v_{2^s})$, with $|v_j| \le 2N$.

(Note that in the above, the $Q(v_{g'})$ is not later than $Q(v_{2^{s-1}})$. That is as it should be, since in the previous heuristic comment, we saw that $g(n-1) = g' \le 2^{s-1}$.)

We are simply trying to bound the number of $(v_1, \ldots, v_{2^s})$ satisfying the above equation. We rewrite that equation as $Q(v_1) + \ldots + Q(v_{g'}) = Z - z$,

where $z = Q(v_{g'+1}) + \ldots + Q(v_{2^{s-1}}) - Q(v_{2^{s-1}+1}) - \ldots - Q(v_{2^s})$.

We will separately bound the M-number of possible z, and the multiplicity with which any Z – z can appear. The bound on $Z = Z_i$ we desire will be the product of those two bounds.

Bounding the M-number of possible z is easy. That M-number is merely the number of $(v_{g'+1}, \ldots, v_{2^{s-1}}, v_{2^{s-1}+1}, \ldots, v_{2^s})$ with each $|v_j| \le 2N$. Thus, each v_j can be chosen in at most

4N + 1 = 5N ways, and so the M-number of possible z is at most $K_{10}N^{2^s - g'}$.

We will now fix a single such z, and bound the multiplicity of $Z - z = Q(v_1) + \ldots + Q(v_{g'})$. The M-number of Z – z (for a fixed z) is just the number of $(v_1, \ldots, v_{g'})$ satisfying $Q(v_1) + \ldots + Q(v_{g'}) = Z - z$, with $|v_j| \le 2N$. Therefore, *by definition*, that M-number is $r_{QN'g'}(Z - z)$, where N′ = 2N. Since g′ = g(n – 1), we will apply our inductive assumption to the degree n – 1 polynomial Q(v), with N′ playing the role of N and $C_{QN'}$ playing the role of C_{PN}. It tells us that

$$r_{QN'g'}(Z - z) \le K(n-1)(C_{QN'})^{F(n-1)}N'^{g'-(n-1)}.$$

We will now replace $C_{QN'}$ with a larger number. We have

$Q(v) = \Phi(h_i, v) = \sum_{u=0}^{n-1} b_u(h_i)v^{(n-1)-u}$. By claim B, $|b_u(h_i)| \le 2^{2n-1}C_{PN}N^u \le 2^{2n-1}C_{PN}N'^u$.

Thus $2^{2n-1}C_{PN} \ge \max\{ \frac{|b_u(h_i)|}{N'^u} \mid 0 \le u \le n-1\} = C_{QN'}$ (the equality by definition of the symbol $C_{QN'}$).

In our earlier inequality, we use $C_{QN'} \le 2^{2n-1}C_{PN}$ and N′ = 2N to see that

$r_{QN'g'}(Z - z) \le K(n-1)(2^{2n-1}C_{PN})^{F(n-1)}N'^{g'-(n-1)} = K_{11}(C_{PN})^{F(n-1)} N^{g'-(n-1)}$.

We have our bound on the multiplicity of Z – z. We multiply that bound our earlier bound on the M-number of possible z, and get $K_{10}K_{11}(C_{PN})^{F(n-1)}N^{2^s - n + 1}$. Letting $K_2 = K_{10}K_{11}$ proves Claim B.

Heuristic remark: We previously mentioned that to make our induction work, we must use C_{PN} in proposition 10, and later replace it with $M_P \ge C_{PN}$ to get the fundamental lemma. We can now see why. The fundamental lemma needs a constant K with $r_{PNg}(m) \le KN^{g-n}$.
The K can depend upon n and P(X), but must not depend upon N. Had we used M_P, then in the inductive step above we would have $r_{QN'g'}(Z - z) \le K(n-1)(M_Q)^{F(n-1)}N'^{g'-(n-1)}$. By definition,

$M_Q = \max\{|b_u(h)| \mid 0 \le u \le n - 1\}$. However, as seen in the proof of claim B, the various $|b_u(h)|$ depend upon N. That would lead to the final K depending upon N.