Definition 1 (Elimination Polynomials). Let p be a prime, $k \in \mathbb{N}$, and $A : \mathrm{Fin}(k+1) \to \mathcal{F}(\mathbb{Z}/p\mathbb{Z})$. We define the elimination polynomials as:

$$g_i(X) = \prod_{a \in A_i} (X_i - a), \quad \forall i \in \mathrm{Fin}(k+1)$$

Definition 2 (Degree Reduction of a Polynomial). Let $P \in \mathrm{MvPoly}(\mathrm{Fin}(k+1), \mathbb{Z}/p\mathbb{Z})$, $g : \mathrm{Fin}(k+1) \to \mathrm{MvPoly}(\mathrm{Fin}(k+1), \mathbb{Z}/p\mathbb{Z})$, and $c : \mathrm{Fin}(k+1) \to \mathbb{N}$. We define the reduced polynomial as:

$$\mathrm{reduce\_polynomial\_degrees}(P, g, c) = \sum_{m \in \mathrm{support}(P)} \begin{cases} \mathrm{coeff}_m(P) \cdot \mathrm{monomial}_{m'} 1 \cdot g_i & \text{if } \exists i, m_i > c_i \\ \mathrm{coeff}_m(P) \cdot \mathrm{monomial}_m 1 & \text{otherwise} \end{cases}$$

where $m' = \mathrm{update}(m, i, m_i - (c_i + 1))$.

Lemma 2.2 (Vanishing on a Product Finset). Let σ be a finite type, R an integral domain, $P \in \mathrm{MvPoly}(\sigma, R)$, and $S : \sigma \to \mathcal{F}(R)$ such that:

1. $\forall i, \mathrm{degreeOf}_i(P) < |S(i)|$

2. $\forall x : \sigma \to R, (\forall i, x_i \in S_i) \Rightarrow \mathrm{eval}_x P = 0$

Then $P = 0$.

Theorem 2.1 (Alon–Nathanson–Ruzsa). Let p be prime, $k \in \mathbb{N}$, and assume:

$h \in \mathrm{MvPoly}(\mathrm{Fin}(k+1), \mathbb{Z}/p\mathbb{Z})$

$A : \mathrm{Fin}(k+1) \to \mathcal{F}(\mathbb{Z}/p\mathbb{Z})$

$c : \mathrm{Fin}(k+1) \to \mathbb{N}$

$\forall i, |A_i| = c_i + 1$

$m = (\sum_i c_i) - \mathrm{totalDegree}(h)$

$\mathrm{coeff}_c \left((\sum_i X_i)^m \cdot h \right) \neq 0$

Define the restricted sumset:

$$S = \left\{ \sum_i f_i : f \in \prod_i A_i, h(f) \neq 0 \right\}$$

Then:

1. $|S| \geq m + 1$

2. $m < p\mathrm{d}$

Proof.

Part 1: Proof that $|S| \geq m + 1$

Assume for contradiction that $|S| \leq m$.

Step 1: Construction of auxiliary set E Since $|S| \leq m$, there exists a multiset E with $S \subseteq E$ and $|E| = m$. Formally, we take $E = S \cup \{\text{zeros}\}$ where we add enough zeros to make the cardinality exactly m.

Step 2: Polynomial construction and vanishing property Define $\text{sumX} = \sum_i X_i$ and $Q = h \cdot \prod_{e \in E}(\text{sumX} - Ce)$.

We prove Q vanishes on $\prod_i A_i$: For any $x \in \prod_i A_i$, if $h(x) \neq 0$ then $\sum_i x_i \in S \subseteq E$, so one factor $(\text{sumX} - C(\sum_i x_i))$ in the product vanishes at x; if $h(x) = 0$ then clearly $Q(x) = 0$.

Step 3: Total degree analysis of Q - THE TECHNICAL HEART OF THE PROOF

We now analyze the total degree of the fundamental building block polynomials.

Theorem: For any $e \in \mathbb{Z}/p\mathbb{Z}$, $\text{totalDegree}(\sum_i X_i - Ce) = 1$.

Proof of upper bound: $\text{totalDegree}(\sum_i X_i - Ce) \leq 1$

We examine the explicit form of the polynomial:

$$P = \sum_i X_i - Ce = X_0 + X_1 + \cdots + X_k - e$$

This is a sum of:

$k + 1$ terms of the form X_i, each being a monomial of total degree 1

One constant term $-e$, which is a monomial of total degree 0

The total degree of a polynomial is defined as the maximum total degree among all monomials with nonzero coefficients in its support. Since all monomials in P have total degree ≤ 1, we immediately conclude that $\text{totalDegree}(P) \leq 1$.

Proof of lower bound: $\text{totalDegree}(\sum_i X_i - Ce) \geq 1$

To prove this, we must demonstrate the existence of at least one monomial of total degree 1 that has a nonzero coefficient in P.

Consider any specific variable X_i. Examine the monomial m_i that consists solely of X_i with exponent 1 (and all other variables with exponent 0). The coefficient of this monomial m_i in P is:

$$\text{coeff}_{m_i}(P) = \text{coeff}_{m_i}(\sum_j X_j) - \text{coeff}_{m_i}(Ce)$$

Now analyze each term:

$\text{coeff}_{m_i}(\sum_j X_j) = 1$, since among all the X_j terms, only X_i contributes to this monomial

$\text{coeff}_{m_i}(Ce) = 0$, because the constant polynomial Ce contains no monomials of positive degree

Therefore, $\text{coeff}_{m_i}(P) = 1 - 0 = 1 \neq 0$.

This proves that the monomial m_i has total degree 1 and appears in P with nonzero coefficient. Hence, $\text{totalDegree}(P) \geq 1$.

Combining both inequalities, we conclude that $\text{totalDegree}(\sum_i X_i - Ce) = 1$.

Step 4: Support structure analysis

Now we analyze the support structure of $P = \sum_i X_i - Ce$.

Theorem: The support of P is contained in $(\bigcup_i \{\text{single}_i 1\}) \cup \{0\}$.

Let d be any monomial in the support of P, meaning $\text{coeff}_d(P) \neq 0$. We have:

$$\text{coeff}_d(P) = \text{coeff}_d(\sum_i X_i) - \text{coeff}_d(Ce) \neq 0$$

We consider cases based on the form of d:

Case 1: $d = \text{single}_i 1$ for some i (a monomial consisting of exactly X_i^1) Then $\text{coeff}_d(\sum_j X_j) = 1$ and $\text{coeff}_d(Ce) = 0$, so $\text{coeff}_d(P) = 1 \neq 0$. Thus $d \in \bigcup_i \{\text{single}_i 1\}$.

Case 2: $d = 0$ (the zero monomial, constant term) Then $\text{coeff}_d(\sum_j X_j) = 0$ and $\text{coeff}_d(Ce) = e$, so $\text{coeff}_d(P) = -e$. If $e \neq 0$, then $\text{coeff}_d(P) \neq 0$, so $d \in \{0\}$.

Case 3: d has any other form If d has total degree ≥ 2, then $\text{coeff}_d(\sum_j X_j) = 0$ and $\text{coeff}_d(Ce) = 0$, so $\text{coeff}_d(P) = 0$. If d has total degree 1 but is not of the form $\text{single}_i 1$, then it must involve at least two different variables with positive exponents, so again $\text{coeff}_d(\sum_j X_j) = 0$ and $\text{coeff}_d(Ce) = 0$.

Therefore, the only monomials with nonzero coefficients in P are those in $(\bigcup_i \{\text{single}_i 1\}) \cup \{0\}$.

Step 5: Degree reduction construction Construct the elimination polynomials $g_i = \prod_{a \in A_i}(X_i - Ca)$ and define $\bar{Q} = \text{reduce\_polynomial\_degrees}(Q, g, c)$.

Step 6: Properties of the reduced polynomial The reduced polynomial $\bar{Q}$ preserves the vanishing property on $\prod_i A_i$, satisfies $\text{degreeOf}_{X_i}(\bar{Q}) \leq c_i$ for all i, and retains the nonzero coefficient of the target monomial.

Step 7: Application of Lemma 2.2 and contradiction Since:

$\bar{Q}$ vanishes on $\prod_i A_i$

$\text{degreeOf}_{X_i}(\bar{Q}) \leq c_i < |A_i|$ for all i (since $|A_i| = c_i + 1$)

By Lemma 2.2, $\bar{Q} = 0$. But the coefficient of $\prod_i X_i^{c_i}$ in $\bar{Q}$ is nonzero, contradiction.

Part 2: Proof that $m < p$ Assume $m \geq p$ for contradiction. In characteristic p, we have the Frobenius identity $(\sum_i X_i)^p = \sum_i X_i^p$.

When $m \geq p$, we can write $(\sum_i X_i)^m$ using the Frobenius map, which redistributes the degrees in a way that makes it impossible for the coefficient of $\prod_i X_i^{c_i}$ in $(\sum_i X_i)^m \cdot h$ to be nonzero, contradicting the hypothesis.

This completes the proof of Theorem 2.1.