令 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$（$p$ 为素数）。

固定整数 $k \geq 0$。对每个 $i \in \{0, \ldots, k\}$ 令 $A_i \subset \mathbb{F}_p$ 且 $|A_i| = c_i + 1$。

设 $h(x_0, \ldots, x_k) \in \mathbb{F}_p[x_0, \ldots, x_k]$ 为一个多项式。记 $\deg(h)$ 为 h 的总次数。

设整数 $m \geq 0$ 满足

$$m + \deg(h) = \sum_{i=0}^{k} c_i.$$

记 $\Sigma(x) := x_0 + \cdots + x_k$（这是你代码里的 'sumX'）。

记向量 $c = (c_0, \ldots, c_k)$；我们关心的目标单项式是 $x^c = x_0^{c_0} \cdots x_k^{c_k}$。

假设给出的代数条件（对应你代码里的 'h$_c$oeff' $[x^c]\big(\Sigma^m \cdot h\big) \neq 0$ （在 $\mathbb{F}_p$ 中）.

定义受限和集

$$S := \big\{\Sigma(a) = a_0 + \cdots + a_k : \ a_i \in A_i, \ h(a) \neq 0\big\}.$$

我们要证明 $|S| \geq m + 1$ 且 $m < p$。

第一部分：证明 $|S| \geq m + 1$

思路概览

若 $|S| \leq m$，把 S 包含进一个大小为 m 的多重集合 $E \subset \mathbb{F}_p$，构造多项式

$$Q(x) := h(x) \cdot \prod_{e \in E} \big(\Sigma(x) - e\big),$$

证明 Q 在 $A_0 \times \cdots \times A_k$ 上处处为零，但通过系数分析得到 Q 的某一指定单项式系数非零，从而矛盾。

下面逐条给出证明中每一条 **Claim** (have)。

Claim 1 (定义 E)

断言：若 $|S| \leq m$，则存在多重集合（或可以视作大小为 m 的列表）$E \subset \mathbb{F}_p$ 使得 $S \subseteq E$ 并 $|E| = m$。

证明：直接取 E 为在集合 S 的元素后补充若干同一元素（例如 0）使得总数为 m。这是纯组合的存在性构造。

Claim 2（定义 Q）

断言：定义

$$Q(x) := h(x) \cdot \prod_{e \in E} \big(\Sigma(x) - e\big).$$

这是我们用于构造矛盾的关键多项式。

Claim 3（Q 在所有 $A_0 \times \cdots \times A_k$ 上为零）

断言：对任意 $x \in A_0 \times \cdots \times A_k$，都有 $Q(x) = 0$。

证明：

若 $h(x) = 0$，显然 $Q(x) = 0$。

若 $h(x) \neq 0$，则 $\Sigma(x) \in S \subseteq E$，因此 $\prod_{e \in E}(\Sigma(x) - e) = 0$。所以 $Q(x) = 0$。

Claim 4（总次数：$\deg P = m$ 和 $\deg Q = \sum c_i$）

令

$$P(x) := \prod_{e \in E}(\Sigma(x) - e).$$

断言 (a)：$\deg(P) = m$。

证明 (a)：每一因子 $\Sigma - e$ 的总次数是 1（因为 Σ 的每项都是度 1 且常数项不改变总度），乘积共有 m 因子，所以总次数为 m。

断言 (b)：因此 $\deg(Q) = \deg(h) + \deg(P) = \deg(h) + m = \sum_{i=0}^{k} c_i$。

Claim 5（把 P 写成 $\Sigma^m + R$，且 $\deg R < m$）

断言：存在多项式 R 使得

$$P = \Sigma^m + R, \quad \text{且} \quad \deg(R) < m.$$

证明：将每个因子 $\Sigma - e$ 展开为 $\Sigma - e$ 并把所有乘出来的最高次项合并得 Σ^m（对应取每个因子中的 Σ 项），其余项每次至少丢失一次 Σ 的选择，从而总次数严格小于 m。

Claim 6（展开 Q 并分析 $[x^c]Q$）

断言：将 $Q = h \cdot P = h\Sigma^m + hR$。我们要计算 $[x^c]Q$。

先看几个子断言。

Claim 6.1 (leading term)：$[x^c]P = [x^c]\Sigma^m$。

证明：任何来自 R 的单项 x^d 满足 $\deg(d) < m$。而为了配出 x^c（其总度为 $\sum c_i = m + \deg(h)$）在乘 h 后贡献到 $[x^c](hP)$ 中，若 h 取的是常数项之外的某个 x^d（$\deg(d) > 0$），则需要 P 为相应的较高度单项来补齐；但 R 的总度 $< m$ 无法为这些情形提供所需的高次度。更直接地说：在 P 的分解中，只有 Σ^m 的高次项可能在乘以 h 后产生总度为 $\sum c_i$ 的项，因此 $[x^c]P = [x^c]\Sigma^m$。

Claim 6.2 (other terms vanish)：若 d 是 h 中的一个非零次数向量（即 $d \neq 0$），则

$$[x^{c-d}]P = 0.$$

证明：$\deg(c-d) = \sum c_i - \deg(d) = m + \deg(h) - \deg(d) > m$ （当 $\deg(d) > 0$ 时），但 P 的最高总度是 m，因此该系数为零。

Claim 6.3（结合）：因此，在计算 $[x^c]Q = [x^c](hP)$ 时，唯一可能非零的乘积项是当 h 取常数项 $[x^0]h$ 时与 $[x^c]P$ 相乘产生的项。所以

$$[x^c]Q = [x^0]h \cdot [x^c]P = [x^0]h \cdot [x^c]\Sigma^m.$$

Claim 7（关于 h 的常数项）

断言：在你的证明框架中通常需要把 h 的常数项当作 1（或至少非零），以保证 $[x^c]Q$ 与 $[x^c]\Sigma^m$ 同非零性相等。我们具体使用的是：$[x^0]h \neq 0$。

说明：你原始的假设给出 $[x^c](\Sigma^m h) \neq 0$。在前面的分解

$$[x^c](\Sigma^m h) = \sum_d [x^d]h \cdot [x^{c-d}]\Sigma^m,$$

当 $[x^{c-d}]\Sigma^m$ 只有在 $d = 0$ 时可能非零（因为 $\deg(\Sigma^m) = m$），可推出 $[x^0]h \cdot [x^c]\Sigma^m \neq 0$。因此必有 $[x^0]h \neq 0$ 且 $[x^c]\Sigma^m \neq 0$。（换句话说，$[x^0]h$ 至少是非零的；若你想把它标准化为 1，可以把 h 除以该非零常数因子。）

Claim 8（因此 $[x^c]Q \neq 0$）

断言：由上面，$[x^c]Q = [x^0]h \cdot [x^c]\Sigma^m \neq 0$。

证明：由 **Claim** 6.3 与 **Claim** 7。

到此我们得出：

Q 在每个 $A_0 \times \cdots \times A_k$ 的点处取值为 0（**Claim** 3），

而 Q 的某个固定单项 x^c 的系数非零（**Claim** 8）。

接下来我们将通过构造一个把变量次数降低到 $\leq c_i$ 的多项式 Q_{bar}，得到同样的矛盾。

Claim 9（定义消元多项式 g_i）

对每个 i 定义

$$g_i(x_i) := \prod_{a \in A_i} (x_i - a).$$

显然 g_i 的次数是 $c_i + 1$，且对任意 $a \in A_i$，$g_i(a) = 0$。

Claim 10（通过替换把 Q 降低至每变量度 $\leq c_i$：定义 Q_{bar}）

构造说明：以如下规则反复替换 Q 中任何出现的 $x_i^{c_i+1}$（或更高次）：用 $g_i(x_i) = x_i^{c_i+1} - (\text{低次项})$

解出

$$x_i^{c_i+1} = (\text{低次项}) \pmod{g_i},$$

把高次项替换为低次项，直到每个变量的出现次数均 $\le c_i$。所得多项式记为 Q_{bar}。

（这是你代码实现 ‘reduce$_p$olynomial$_d$egrees‘

Claim 11（替换不改变在 $A_0 \times \cdots \times A_k$ 上的值）

断言：对于任意 $x \in A_0 \times \cdots \times A_k$，都有 $Q_{\text{bar}}(x) = Q(x) = 0$。

证明：每一次替换规则都是用恒等式

$$x_i^{c_i+1} - (\text{低次多项}) = g_i(x_i),$$

对多项式做代换；在点 x 上，如果 $x_i \in A_i$ 则 $g_i(x_i) = 0$。因此每一次替换都在这些点上保持多项式取相同的值。既然初始的 $Q(x) = 0$，替换后仍为 0。

Claim 12（替换后每个变量的次数受限）

断言：Q_{bar} 对每个 i 满足 $\deg_{x_i} Q_{\text{bar}} \le c_i$。

证明：替换规则的目的是消除所有指数超过 c_i 的幂，因此最终得到的多项式每个变量次数至多 c_i。

Claim 13（应用组合 Nullstellensatz / 逐变量度控制的消失引理）

引理（多变量版）：设 $P \in \mathbb{F}_p[x_0, \ldots, x_k]$。若对每个 i，$\deg_{x_i} P < |A_i|$，且 P 在 $A_0 \times \cdots \times A_k$ 的所有点上均取零值，则 P 为零多项式。

应用：由于 $|A_i| = c_i + 1$ 且 $\deg_{x_i} Q_{\text{bar}} \le c_i$，我们有 $\deg_{x_i} Q_{\text{bar}} < |A_i|$。再加上 **Claim** 11（在笛卡尔积上处处为 0），由引理可得：

断言：$Q_{\text{bar}} = 0$。

Claim 14（替换过程不改变目标系数）

断言：替换过程中不会改变 x^c 的系数，所以

$$[x^c]Q_{\text{bar}} = [x^c]Q \neq 0.$$

证明：在替换过程中，任何一次用 $x_i^{c_i+1} =$（低次项）替换都会把某个指数分量 $\ge c_i + 1$ 的单项替为若干单项，这些新单项在该变量方向的指数都 $\le c_i$。因此目标单项 x^c（在每个分量刚好是 c_i）不会被“生成”自替换的结果；反过来，也不会被替换为别的项而丢失——更精确地说：替换只会把具有某个变量指数 $> c_i$ 的单项写成若干次幂中指数 $\le c_i$ 的线性组合，但这些替换不会改变原来那一项 x^c 的系数，因为 x^c 本身的每个分量都不超过 c_i，即替换不会触及已经恰好等于上限的幂。形

式化可以通过追踪替换过程中每一步对目标单项系数的影响来完成（每一步对目标单项系数的改变量均为 0）。

矛盾：由 **Claim** 13 我们有 $Q_{\text{bar}} = 0$，但由 **Claim** 14 我们有 $[x^c]Q_{\text{bar}} \neq 0$。矛盾。

因此假设 $|S| \leq m$ 必为假的，从而得出

$$\boxed{|S| \geq m + 1.}$$

这是第一部分结论。

第二部分：证明 $m < p$

我们现在证明 $m < p$。思路是：如果 $m \geq p$，利用特征 p 下的“Freshman's dream”与指数模 p 的整除性质，结合每个 $c_i \leq p - 1$（因为 $c_i + 1 = |A_i| \leq p$，集合 $A_i \subset \mathbb{F}_p$ 的大小至多 p）得到与前面关于系数非零的断言矛盾。

下面详细写出每一步 have。

Claim 15（每个 c_i 小于 p）

断言：对每个 i，$0 \leq c_i \leq p - 1$。

证明：因为 $A_i \subset \mathbb{F}_p$，所以 $|A_i| \leq p$。由 $|A_i| = c_i + 1$ 得 $c_i \leq p - 1$。显然 $c_i \geq 0$。

假设反面并写 $m = pq + r$

假设 $m \geq p$。将 m 写成 $m = pq + r$ 其中 $q \geq 1$ 且 $0 \leq r \leq p - 1$（这是整除带余数分解）。

Claim 16（$\Sigma^p = \sum_i x_i^p$ 在特征 p 下）

断言：

$$(\Sigma)^p = (x_0 + \cdots + x_k)^p = x_0^p + \cdots + x_k^p.$$

证明：在特征 p 的域中，二项式（多项式）的中间项都乘以二项式系数 $\binom{p}{j}$（$0 < j < p$），而这些系数都被 p 整除，故在 $\mathbb{F}_p$ 中为零。因此展开只剩下 x_i^p 项之和。

Claim 17（形式分解 $\Sigma^m = (\Sigma^p)^q \cdot \Sigma^r$）

断言：

$$\Sigma^m = (\Sigma^p)^q \cdot \Sigma^r = \Big(\sum_{i=0}^{k} x_i^p\Big)^q \cdot \Sigma^r.$$

这是代数上直接成立的幂的分解。

Claim 18（每个单项在 $(\sum x_i^p)^q$ 中的指数都能被 p 整除）

断言：任一出现在 $(\sum_i x_i^p)^q$ 展开中的单项形如 $\prod_i x_i^{p \cdot t_i}$（也就是每个变量的指数均为 p 的倍数）。

证明：显然，因为每项来自若干次选取 x_j^p 因子并相乘，指数是 p 的倍数。

Claim 19（若 $c_i < p$ 中某些 c_i 非零，则 $[x^c](\Sigma^{pq}) = 0$）

断言：由于 $c_i < p$（**Claim** 15），在 $(\sum x_i^p)^q$ 中不可能出现指数恰好等于 $c = (c_0, \ldots, c_k)$（除非 $c = 0$），因此 $[x^c](\Sigma^{pq}) = 0$。

证明：任一单项在 $(\sum x_i^p)^q$ 中每个分量都是 p 的倍数，而 $0 \le c_i \le p-1$；若某 $c_i \neq 0$（或任一 c_i 不是 p 的倍数，显然），就无法匹配一个每分量为 p-倍数的向量，故系数为 0。注意 c 的总度 $\sum c_i = m + \deg(h) \ge m \ge p$，所以 c 不是全零向量，因此至少有一个分量大于 0。

Claim 20（结合 $\Sigma^m = (\Sigma^{pq})\Sigma^r$ 得到 $[x^c]\Sigma^m = 0$）

断言：在上述分解中，$[x^c]\Sigma^m = 0$。

证明：任何单项 x^c 若要在乘积中出现，必须是从某个单项 x^u（来自 $(\sum x_i^p)^q$）和某个单项 x^v（来自 Σ^r）相乘得到，且 $u + v = c$。但 u 的每个分量是 p 的倍数，而 v 的总度是 $r < p$。因此 u 的总度至少是 0 并且是 p 的倍数；而 $\sum c_i = \sum u_i + \sum v_i$。由于 $\sum v_i = r < p$ 且 $\sum c_i \ge m \ge p$，必须有 $\sum u_i \ge p$。但 $\sum u_i$ 是 p 的倍数，因此至少为 p。若要满足每个分量 u_i 都为 p 倍，而 $c_i < p$（每个分量 $< p$），那意味着 u_i 必须全部为 0。然而若所有 $u_i = 0$，则 $v = c$ 并且 $\sum v_i = \sum c_i \ge p$，这与 $\sum v_i = r < p$ 矛盾。因此不存在这样的分解，故 $[x^c]\Sigma^m = 0$。

（这一点需要细心检验：核心思想是指数的模 p 性质与总度大小的不兼容；因为 u 每个分量被 p 整除而 c 每个分量都在 $0, \ldots, p-1$ 之间，矛盾产生。）

Claim 21（与先前关于 $[x^c](\Sigma^m h) \neq 0$ 矛盾）

断言：若 $[x^c]\Sigma^m = 0$，则对所有 d 有 $[x^{c-d}]\Sigma^m = 0$（因为 $\deg(\Sigma^m) = m$，可用同类理由），从而

$$[x^c](\Sigma^m h) = \sum_d [x^d]h \cdot [x^{c-d}]\Sigma^m = 0,$$

与初始假设 $[x^c](\Sigma^m h) \neq 0$ 矛盾。

因此假设 $m \ge p$ 导致矛盾，故必有

$$\boxed{m < p.}$$

结论

综合两部分结果，我们得出在给定假设下（特别是假设 $[x^c](\Sigma^m h) \neq 0$ 且 $|A_i| = c_i + 1$）：

$|S| \ge m + 1$，

$m < p$。

这正是你代码欲证明的结论（ANR 多项式方法的要点）。

进一步说明与可选证明细节

1. 关于 **Claim** 6 的严格性：上面对“其他项为 0”的论证用了“总次数的比较”这一直观但严谨的方式；形式化时可以以“如果 h 取非零次数向量 $d \neq 0$ 则 $\deg(c-d) > \deg(P) = m$ ”为线索，逐项说明相应系数在 P 中为 0。

2. 关于替换不改变目标系数（**Claim** 14）：形式化证明可以用归纳：考虑一个单次替换 $x_i^t \mapsto x_i^{t-(c_i+1)} \cdot g_i(x_i)$ 的反写，追踪目标单项在替换前后系数的变化，证明不会影响恰好指数为 c 的项。或者更简洁地把替换视为在多项式环里把 Q 映射到商环

$$\mathbb{F}_p[x_0, \ldots, x_k]/(g_0, \ldots, g_k)$$

中的代表；在该商环里，每个 $x_i^{c_i+1}$ 被替换为低次多项，从而 Q 在代表类中与 Q_{bar} 一致，而 x^c 为该商环中仍然代表一个非零基向量（因为 $c_i \leq p-1$ 并且 x^c 的系数在商环中被保留），所以在系数层面不变。

3. 关于第二部分（$m < p$）的关键点：要点是 $c_i < p$（每个分量小于 p），而在 $(\sum x_i^p)^q$ 中出现的所有指数分量都是 p 的倍数，因此不可能拼凑出每分量都位于 $0, \ldots, p-1$ 的 c。这类模 p 的指数-余数考虑是特征 p 微妙但强有力的工具。