Polynomials and Codes

Aart Blokhuis
TU/e Eindhoven

13 September, 2012, Trieste
ICTP-IPM Workshop and Conference
in Combinatorics and Graph Theory.
Reza and Richard: Thanks for a wonderful meeting.

From now on: p is prime and q is a power of p.

Codes

A *q-ary linear* $[n, k, d]$*-code* C is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$, of ordered n-tuples from the finite field of order q, such that the minimum weight of a nonzero vector in the code (a codeword) is d.

Codes

A *q-ary linear* $[n, k, d]$*-code* C is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$, of ordered n-tuples from the finite field of order q, such that the minimum weight of a nonzero vector in the code (a codeword) is d.

The *Hamming-distance* between two vectors u and v is the number of coordinates in which they differ.

The weight of u is the number of nonzero coordinates, so the Hamming-distance of u to the origin.

Codes

A q-*ary linear* $[n, k, d]$-*code* C is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$, of ordered n-tuples from the finite field of order q, such that the minimum weight of a nonzero vector in the code (a codeword) is d.

The *Hamming-distance* between two vectors u and v is the number of coordinates in which they differ.

The weight of u is the number of nonzero coordinates, so the Hamming-distance of u to the origin.

A vector of weight 3 in $\mathbb{F}_3^5$: $u = (0, 1, 0, 2, 1)$.

Codes

A q-*ary linear* $[n, k, d]$-*code* C is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$, of ordered n-tuples from the finite field of order q, such that the minimum weight of a nonzero vector in the code (a codeword) is d.

The *Hamming-distance* between two vectors u and v is the number of coordinates in which they differ.

The weight of u is the number of nonzero coordinates, so the Hamming-distance of u to the origin.

A vector of weight 3 in $\mathbb{F}_3^5$: $u = (0, 1, 0, 2, 1)$.

Central problem: For which $[n, k, d]$ does a q-ary code exist.

Codes

A q-*ary linear* $[n, k, d]$-*code* C is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$, of ordered n-tuples from the finite field of order q, such that the minimum weight of a nonzero vector in the code (a codeword) is d.

The *Hamming-distance* between two vectors u and v is the number of coordinates in which they differ.

The weight of u is the number of nonzero coordinates, so the Hamming-distance of u to the origin.

A vector of weight 3 in $\mathbb{F}_3^5$: $u = (0, 1, 0, 2, 1)$.

Central problem: For which $[n, k, d]$ does a q-ary code exist.

Example: the Griesmer-bound: $n \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil$.

The Generator Matrix

A linear $[n, k, d]$-code can be represented as the row space of a $k \times n$ matrix G of rank k. Such a matrix is called a *generator matrix* of the code.

The Generator Matrix

A linear $[n, k, d]$-code can be represented as the row space of a $k \times n$ matrix G of rank k. Such a matrix is called a *generator matrix* of the code.

Codewords are all vectors xG, $x \in \mathbb{F}_q^k$. We can also view xG as the list of inner products of x with the columns of G. When we view the columns of G as vectors in $\mathbb{F}_q^k$, or better, as points in $\mathcal{P} = PG(k-1, q)$, and x as a vector defining a hyperplane we find corresponding to the code a (multi-)set S of n points in $\mathcal{P}$ having at most $n - d$ points in every hyperplane.

The Generator Matrix

A linear $[n, k, d]$-code can be represented as the row space of a $k \times n$ matrix G of rank k. Such a matrix is called a *generator matrix* of the code.

Codewords are all vectors xG, $x \in \mathbb{F}_q^k$. We can also view xG as the list of inner products of x with the columns of G. When we view the columns of G as vectors in $\mathbb{F}_q^k$, or better, as points in $\mathcal{P} = PG(k-1, q)$, and x as a vector defining a hyperplane we find corresponding to the code a (multi-)set S of n points in $\mathcal{P}$ having at most $n - d$ points in every hyperplane.

This correspondence goes both ways.
Exercise: Prove the Griesmer-bound (by induction).

First example

$\mathbb{F}_3 = \{0, 1, 2\}$ arithmetic mod 3,

$$G = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

is the generator matrix of a ternary $[9, 3, 6]$ code (every hyperplane contains at most 3 columns, so $d = 6$). The Griesmer-bound gives $n \geq 6 + 6/3 + \lceil 6/9 \rceil = 9$, so we have equality.

First example

$\mathbb{F}_3 = \{0, 1, 2\}$ arithmetic mod 3,

$$G = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

is the generator matrix of a ternary $[9, 3, 6]$ code (every hyperplane contains at most 3 columns, so $d = 6$). The Griesmer-bound gives $n \geq 6 + 6/3 + \lceil 6/9 \rceil = 9$, so we have equality.

The set S consists of all points of $AG(2, 3)$.

Second example

$\mathbb{F}_4 = \{0, 1, a, a^2\}$ arithmetic mod 2, $a^3 = a^2 + a = 1$.

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & a & a^2 & 0 & 1 \\ 0 & 1 & a^2 & a & 1 & 0 \end{pmatrix}$$

or, essentially equivalent

$$G_2 = \begin{pmatrix} 0 & 1 & a & 1 & 0 & a \\ 0 & a & 1 & 1 & a & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

are generator matrices of quaternary $[6, 3, 4]$ codes. The Griesmer-bound gives $n \geq 4 + 4/4 + \lfloor 4/16 \rfloor = 6$.

Second example

$\mathbb{F}_4 = \{0, 1, a, a^2\}$ arithmetic mod 2, $a^3 = a^2 + a = 1$.

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & a & a^2 & 0 & 1 \\ 0 & 1 & a^2 & a & 1 & 0 \end{pmatrix}$$

or, essentially equivalent

$$G_2 = \begin{pmatrix} 0 & 1 & a & 1 & 0 & a \\ 0 & a & 1 & 1 & a & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

are generator matrices of quaternary $[6, 3, 4]$ codes. The Griesmer-bound gives $n \geq 4 + 4/4 + \lfloor 4/16 \rfloor = 6$.

The set S_1 is a hyperoval in $PG(2, 4)$ (and S_2 in $AG(2, 4)$).

If weights and length have a common divisor

Suppose there is an r dividing n and all weights, and that the columns of G are (projectively) different. So we get a set S of points in $\mathcal{P} = PG(k-1, q)$ intersecting every hyperplane in a multiple of r points.

If weights and length have a common divisor

Suppose there is an r dividing n and all weights, and that the columns of G are (projectively) different. So we get a set S of points in $\mathcal{P} = PG(k-1, q)$ intersecting every hyperplane in a multiple of r points.

A very annoying problem: Let S be a set of p^2 points in $AG(3, p)$ (or $PG(3, p)$) which intersects every plane in 0 mod p points, does it follow that S is a cylinder, the union of p parallel lines (or, in the projective version a cone with the top removed)?

Point sets in the plane, $k = 3$.

Theorem

A set of points S in $PG(2, q)$ which is incident with 0 mod r points of every line has at least $(r-1)q + (p-1)r$ points, where $1 < r < q = p^h$.

Point sets in the plane, $k = 3$.

Theorem

A set of points S in $PG(2, q)$ which is incident with 0 mod r points of every line has at least $(r-1)q + (p-1)r$ points, where $1 < r < q = p^h$.

A maximal r-arc in $PG(2, q)$ is a set S intersecting every line in 0 or r points. For q odd and $1 < r < q$ maximal arcs don't exist (Ball, B. and Mazzocca '97) the above result strengthens this: $(r-1)q + r < (r-1)q + (p-1)r$ for $p > 2$.

The proof uses the *maximal arcs polynomial*, the next slides gives a flavour of the proof.

The maximal arcs polynomial, I

The story begins with the (proof of the) following:

Theorem (B., Wilbrink '87)

*Let B be a set of $q+1$ points in $AG(2,q)$, and let A be a set of points (*nuclei*) such that every line containing a point of A contains a (unique) point of B. Then $|A| \leq q-1$.*

The maximal arcs polynomial, I

The story begins with the (proof of the) following:

Theorem (B., Wilbrink '87)

*Let B be a set of $q+1$ points in $AG(2,q)$, and let A be a set of points (*nuclei*) such that every line containing a point of A contains a (unique) point of B. Then $|A| \leq q-1$.*

Step 1: Identify $AG(2,q)$ with $\mathbb{F}_{q^2}$.
Step 2: a, b and c are collinear iff $(a-b)^{q-1} = (a-c)^{q-1}$.
Step 3: Associate to B the polynomial
$\mathcal{B}(Y) = \sum_{b \in \mathcal{B}} (Y-b)^{q-1}$.
Step 4: Show that points of A are zeros of the polynomial $\mathcal{B}$.

The maximal arcs polynomial, II

The next step came from (the proof of) the following:

Theorem

Let S be a set of $q+n$ points in $AG(2,q)$, and let A be a set of points such that every line containing a point of A contains at least one point of S. Then $|A| \leq n(q-1)$.

The maximal arcs polynomial, II

The next step came from (the proof of) the following:

Theorem

Let S be a set of $q+n$ points in $AG(2,q)$, and let A be a set of points such that every line containing a point of A contains at least one point of S. Then $|A| \leq n(q-1)$.

Step 3': Associate to S the polynomial $R(X,Y) = \prod_{b \in S}(X-(Y-b)^{q-1}) = \sum_{j=0}^{|S|} \sigma_j(Y) X^{|S|-j}$.
Step 4': Show that points of A are zeros of the 'coefficientpolynomial' $\sigma_n(Y)$ of degree $n(q-1)$: use that $R(X,a)$ is divisible by $(X^{q+1}-1)$.

Back to point sets in the plane.

Theorem (Ball, B., Gács, Sziklai, Weiner, 2007)

A set of points S in $PG(2,q)$ which is incident with 0 mod r points of every line has at least $(r-1)q+(p-1)r$ points, where $1<r<q=p^h$.

Back to point sets in the plane.

Theorem (Ball, B., Gács, Sziklai, Weiner, 2007)

A set of points S in $PG(2,q)$ which is incident with 0 mod r points of every line has at least $(r-1)q+(p-1)r$ points, where $1<r<q=p^h$.

Step 0: Show that you may take S in $AG(2,q)$.
Step 3': Associate to S the polynomial
$R(X,Y)=\prod_{b\in S}(X-(Y-b)^{q-1})=\sum_{j=0}^{|S|}\sigma_j(Y)X^{|S|-j}$.
Step 4": Use that $R(X,y)$ is divisible by $X(X^{q+1}-1)^{r-1}$ for $y\in S$ and that $R(X,y)$ is an r-th power for $y\notin S$.
Step 5: Think for a couple of years, and finish the proof.

Coding theory again

In terms of coding theory this reads as follows, where the dual minimum distance of a code is the minimum distance of the dual code, $C^{\perp}$. The condition that the dimension is 3 can in fact be deleted, but this takes some extra effort.

Theorem (BBGSzW)

A code of dimension 3 whose weights and length have a common divisor $1 < r < q$ and whose dual minimum distance is at least 3 has length at least $(r-1)q + (p-1)r$.

Picture time I

Here are Péter Sziklai, András Gács (and my wife Ágnes).

Picture time II

And here we have the Ball family, and Zsuzsa Weiner.

Picture time III

Franco Mazzocca (on the right):

Another problem, another polynomial.

Let again C be a q-ary $[n, k, d]$-code, given n, k we want to maximize d or given n, d we want to maximize k, or given k, d we want to minimize n. In wat follows we will give bounds for d in terms of m, the maximal weight of a codeword. Normally m will be close to n of course, but we will only assume $m \geq n - d + 1$, for otherwize, by adding the all-one word we make k larger without decreasing d.

The general result is rather technical, and it's usefulness will only be illustrated in a number of special cases. In the next slide we'll state the (also rather technical) special case that $q(= p)$, the order of the field, is a prime.

A bound for the maximum weight

Theorem (Ball, B. 2012)

Let C be a p-ary $[n, k, d]$-code with a word of weight m, then $m \leq (n-d)p - e(p-1)$, where $0 \leq e \leq k-2$ satisfies $\binom{n-d}{e} \neq 0 \pmod{p^{k-1-e}}$.

In particular, if C contains a codeword of weight n, then $n \geq d/(p-1) + d + e$.

A bound for the maximum weight

Theorem (Ball, B. 2012)

Let C be a p-ary $[n, k, d]$-code with a word of weight m, then $m \leq (n-d)p - e(p-1)$, where $0 \leq e \leq k-2$ satisfies $\binom{n-d}{e} \neq 0 \pmod{p^{k-1-e}}$.
In particular, if C contains a codeword of weight n, then $n \geq d/(p-1) + d + e$.

Let us recall the Griesmer-bound: $n \geq \sum_{i=0}^{k-1} \lceil d/p^i \rceil$.

Polynomials again

Where does this strange condition with the binomial coefficient come from?

Polynomials again

Where does this strange condition with the binomial coefficient come from?

What we prove in fact is that:

If there is a q-ary $[n, k, d]$-code with maximum weight $m \geq n - d + 1$,

then for all $\epsilon \geq 1$, the coefficient of $X^{(n-d)q-m+\epsilon}$ in the *real* polynomial, or better, formal power series,

$$(1 + X)^{-m}(1 + X^p)^{(n-d)q/p}$$

is divisible by q^{k-1}.

Why is this useful (and interesting) ?

When we translate the results back to statements about point sets S in projective or affine space we obtain (in many cases improved) bounds for (n, t)-arcs and t-fold blocking sets of hyperplanes in $AG(k-1, q)$.

Why is this useful (and interesting) ?

When we translate the results back to statements about point sets S in projective or affine space we obtain (in many cases improved) bounds for (n, t)-arcs and t-fold blocking sets of hyperplanes in $AG(k-1, q)$.

The best existing bounds in these cases were also obtained using polynomials, either the Rédei-polynomial or the maximal arcs polynomial, but these are polynomials with coefficients in a finite field, and at some point binomial coefficients vanish, and so does the use of the polynomial. The difference is that this time we look at real polynomials and formal power series.

Intermezzo: A curious hypercongruence.

A curious byproduct of our investigations is the following hypercongruence: The sum

$$\sum_{k=0}^{p-1} \binom{p^3+p^2-p-1}{p^2-p-pk} \binom{-p^2}{k}$$

is (exactly) divisible by p^{p+1} (more precisely, it equals $-p^{p+1}$ mod p^{p+4}). A nice one for your advanced problem solving course.

Application I: Arcs in affine space

An (n, t)-arc is a set S of size n with at most t points in a hyperplane.

Application I: Arcs in affine space

An (n, t)-arc is a set S of size n with at most t points in a hyperplane.

Theorem

If there is an (n, t)-arc in $AG(s, q)$, then for all $\epsilon \geq 1$ the coefficient of $X^{tq-n+\epsilon}$ in $(1+X)^{-n}(1+X^p)^{tq/p}$ is divisible by q^s.

Application I: Arcs in affine space

An (n, t)-arc is a set S of size n with at most t points in a hyperplane.

Theorem

If there is an (n, t)-arc in $AG(s, q)$, then for all $\epsilon \geq 1$ the coefficient of $X^{tq-n+\epsilon}$ in $(1+X)^{-n}(1+X^p)^{tq/p}$ is divisible by q^s.

Theorem

If there is an (n, t)-arc in $AG(s, p)$, then $n \leq (t-e)p + e$, where $0 \leq e < s$ and $\binom{t}{e} \neq 0 \pmod{p^{s-e}}$.

Application I: Arcs in the affine plane

An (n, t)-arc in the plane is a set S of size n with at most t points on a line.

Application I: Arcs in the affine plane

An (n, t)-arc in the plane is a set S of size n with at most t points on a line.

Theorem

If there is an (n, t)-arc in $AG(2, q)$, then for all $\epsilon \geq 1$ the coefficient of $X^{tq-n+\epsilon}$ in $(1+X)^{-n}(1+X^p)^{tq/p}$ is divisible by q^2.

Application I: Arcs in the affine plane

An (n, t)-arc in the plane is a set S of size n with at most t points on a line.

Theorem

If there is an (n, t)-arc in $AG(2, q)$, then for all $\epsilon \geq 1$ the coefficient of $X^{tq-n+\epsilon}$ in $(1+X)^{-n}(1+X^p)^{tq/p}$ is divisible by q^2.

Theorem

If there is an (n, t)-arc in $AG(2, p)$, then $n \leq (t-e)p + e$, where $0 \leq e < 2$ and $\binom{t}{e} \neq 0 \pmod{p^{2-e}}$.

Application II: Blocking sets in affine space

A t-fold blocking set (of hyperplanes) is a set B with at least t points in a hyperplane, the complement of a $|H| - t$-arc.

Theorem

If S is a t-fold blocking set of $AG(s, q)$, then for all $\epsilon \geq 1$ the coefficient of $X^{|S|-tq+\epsilon}$ in $(1+X)^{|S|-q^s}(1+X^p)^{(q^{s-1}-t)q/p}$ is divisible by q^s.

Application II: Blocking sets in affine space

A t-fold blocking set (of hyperplanes) is a set B with at least t points in a hyperplane, the complement of a $|H| - t$-arc.

Theorem

If S is a t-fold blocking set of $AG(s, q)$, then for all $\epsilon \geq 1$ the coefficient of $X^{|S|-tq+\epsilon}$ in $(1+X)^{|S|-q^s}(1+X^p)^{(q^{s-1}-t)q/p}$ is divisible by q^s.

Theorem

If S is a t-fold blocking set in $AG(s, p)$, then $|S| \geq (t+e)p - e$, where $0 \leq e < s$ and $\binom{-t}{e} \neq 0 \pmod{p^{s-e}}$.

Application II: Blocking sets in affine space

A t-fold blocking set in the plane is a set B with at least t points on every line, the complement of a $|H| - t$-arc.

Theorem

If S is a t-fold blocking set of $AG(2, q)$, then for all $\epsilon \geq 1$ the coefficient of $X^{|S|-tq+\epsilon}$ in $(1+X)^{|S|-q^2}(1+X^p)^{(q^{2-1}-t)q/p}$ is divisible by q^2.

Application II: Blocking sets in affine space

A t-fold blocking set in the plane is a set B with at least t points on every line, the complement of a $|H| - t$-arc.

Theorem

If S is a t-fold blocking set of $AG(2, q)$, then for all $\epsilon \geq 1$ the coefficient of $X^{|S|-tq+\epsilon}$ in $(1+X)^{|S|-q^2}(1+X^p)^{(q^{2-1}-t)q/p}$ is divisible by q^2.

Theorem

If S is a t-fold blocking set in $AG(2, p)$, then $|S| \geq (t+e)p - e$, where $0 \leq e < 2$ and $\binom{-t}{e} \neq 0 \pmod{p^{2-e}}$.

Some history, the Rédei polynomial

Let S be a set of points in $AG(2,q)$. The Rédei polynomial associated to S is the product:

$$R(T,V_1,V_2)=\prod_{u\in S}(T+u_1V_1+u_2V_2).$$

If $v_1X_1+v_2X_2=c$ stands for a parallel class of lines, then the specialization

$$R(T,v_1,v_2)=\prod_{u\in S}(T+u_1v_1+u_2v_2)=\prod_{c\in\mathbb{F}_q}(T+c)^{m(c)},$$

where $m(c)$ counts the number of points of S on the line $v_1X_1+v_2X_2=c$.

Some history, the Rédei polynomial

Let S be a set of points in $AG(2,q)$. The Rédei polynomial associated to S is the product:

$$R(T,V_1,V_2)=\prod_{u\in S}(T+u_1V_1+u_2V_2).$$

If $v_1X_1+v_2X_2=c$ stands for a parallel class of lines, then the specialization

$$R(T,v_1,v_2)=\prod_{u\in S}(T+u_1v_1+u_2v_2)=\prod_{c\in\mathbb{F}_q}(T+c)^{m(c)},$$

where $m(c)$ counts the number of points of S on the line $v_1X_1+v_2X_2=c$.

This polynomial is extremely useful for the study of blocking sets and directions, but: it is defined over $\mathbb{F}_q$, so sometimes coefficients vanish because binomial coefficients are zero.

Thank you Rédei!

Intermezzo: Group characters

$G = (\mathbb{F}_q^{k-1}, +, 0)$ the additive group of the vector space, $\hat{G}$ the (multiplicative) group of characters, explicitly:
$\hat{G} = \{\chi_u \mid u \in G\}$, with $\chi_u(x) = \exp(2\pi i \mathrm{Tr}(x \cdot u)/p)$, where Tr is the tracefunction from $\mathbb{F}_q$ to $\mathbb{F}_p$.

Lemma

Let $g(x) = \sum_{\chi \in \hat{G}} c_\chi \chi(x)$, *where* $c_\chi \in \mathbb{Z}$. *If* $g(x) = 0$ *for all* $x \in G \setminus \{0\}$, *then* q^{k-1} *divides* $g(0)$.

The oneline proof:

$$g(0) = \sum_{x \in G} g(x) = \sum_{x \in G} \sum_{\chi \in \hat{G}} c_\chi \chi(x) = \sum_{\chi \in \hat{G}} \sum_{x \in G} \chi(x) = c_{\chi_0} |G|.$$

Group characters, the case $q = p$, prime

$G = (\mathbb{F}_p^{k-1}, +, 0)$ the additive group of the vector space, $\hat{G}$ the (multiplicative) group of characters, explicitly:
$\hat{G} = \{\chi_u \mid u \in G\}$, with $\chi_u(x) = \eta^{x \cdot u}, \quad \eta = \exp 2\pi i/p$

Lemma

Let $g(x) = \sum_{\chi \in \hat{G}} c_\chi \chi(x)$, *where* $c_\chi \in \mathbb{Z}$. *If* $g(x) = 0$ *for all* $x \in G \setminus \{0\}$, *then* p^{k-1} *divides* $g(0)$.

Polynomial time again

On the background we have a p-ary $[n, k, d]$-code C, containing a word of (full) weight n, say the all one word. If we put this as the last row in the generator matrix G, then the columns define a set $S \subset AG(k-1, p) \simeq \mathbb{F}_p^{k-1} \simeq G$. We associate to C, or better to the point set S the following quasi-polynomial ($\eta = \exp(2\pi i/p)$):

$$f(X, x) = \prod_{u \in S}(X + \chi_u(x)) = \prod_{u \in S}(X + \eta^{u \cdot x}).$$

So for every $x \in G$ this defines a polynomial in $\mathbb{C}[X]$.

$f(X,x) = \prod_{u \in S}(X + \chi_u(x))$; $\chi_u(x) = \eta^{x \cdot u}$; $\eta = \exp(2\pi i/p)$.

We may define a formal inverse $g(X,x) = \sum_{j=0}^{\infty} g_j(x) X^j$,

satisfying $f(X,x)G(X,x) = 1$.

The 'coefficients' g_j will be integral linear combinations of characters: $g_j(x) = \sum_{\chi \in \hat{G}} c_\chi \chi(x)$, and $c_\chi \in \mathbb{Z}$.

$f(X,x) = \prod_{u \in S}(X + \chi_u(x))$; $\chi_u(x) = \eta^{x \cdot u}$; $\eta = \exp(2\pi i/p)$.

We may define a formal inverse $g(X,x) = \sum_{j=0}^{\infty} g_j(x) X^j$,

satisfying $f(X,x)G(X,x) = 1$.

The 'coefficients' g_j will be integral linear combinations of characters: $g_j(x) = \sum_{\chi \in \hat{G}} c_\chi \chi(x)$, and $c_\chi \in \mathbb{Z}$.

$f(X,0) = (X+1)^n$, and for $x_0 \neq 0$ the multi-set $\{\chi_u(x_0) \mid u \in S\}$ contains each p-th root of unity at most $(n-d)q/p$ times, so $f(X,x_0) \mid (X^p+1)^{\gamma q/p}$ if $\gamma \geq n-d$.

$$f(X,x) = \prod_{u\in S}(X + \chi_u(x)) = \prod_{u\in S}(X + \eta^{u\cdot x};$$

We may define a formal inverse $g(X,x) = \sum_{j=0}^{\infty} g_j(x)X^j$,

satisfying $f(X,x)G(X,x) = 1$.

The 'coefficients' g_j will be integral linear combinations of characters: $g_j(x) = \sum_{\chi\in\hat{G}} c_\chi\chi(x)$, and $c_\chi \in \mathbb{Z}$.

$f(X,x) = \prod_{u \in S}(X + \chi_u(x)) = \prod_{u \in S}(X + \eta^{u \cdot x};$

We may define a formal inverse $g(X,x) = \sum_{j=0}^{\infty} g_j(x) X^j$,

satisfying $f(X,x)G(X,x) = 1$.

The 'coefficients' g_j will be integral linear combinations of characters: $g_j(x) = \sum_{\chi \in \hat{G}} c_\chi \chi(x)$, and $c_\chi \in \mathbb{Z}$.

$f(X,0) = (X+1)^n$, and for $x_0 \neq 0$ the multi-set $\{\chi_u(x_0) \mid u \in S\}$ contains each p-th root of unity at most $(n-d)$ times, in other words, the multi-set $\{u \cdot x_0 \mid u \in S\}$ contains every number $0, 1, \ldots, p-1$ at most $(n-d)$ times so $f(X,x_0) \mid (X^p+1)^\gamma$ if $\gamma \geq n-d$.

The last slide!

$f(X,0) = (X+1)^n$, and for $x_0 \neq 0$ the multi-set $\{\chi_u(x_0) \mid u \in S\}$ contains each p-th root of unity at most $(n-d)q/p$ times, so $f(X,x_0) \mid (X^p+1)^{\gamma q/p}$ if $\gamma \geq n-d$.

The last slide!

$f(X,0) = (X+1)^n$, and for $x_0 \neq 0$ the multi-set $\{\chi_u(x_0) \mid u \in S\}$ contains each p-th root of unity at most $(n-d)q/p$ times, so $f(X,x_0) \mid (X^p+1)^{\gamma q/p}$ if $\gamma \geq n-d$.

It follows that $h(X,x) := (X^p+1)^{\gamma q/p} g(X,x)$ is a polynomial of degree $\gamma q/p - n$ for each $x \in G \setminus \{0\}$, finally in the formal power series $h(X,0) = (1+X)^{-n}(1+X^p)^{\gamma q/p}$ the coefficients of all $X^{>\gamma q/p-n}$ are divisible by q^{k-1} by the characterlemma.

The last slide!

$f(X,0) = (X+1)^n$, and for $x_0 \neq 0$ the multi-set $\{\chi_u(x_0) \mid u \in S\}$ contains each p-th root of unity at most $(n-d)$ times, so $f(X,x_0) \mid (X^p+1)^\gamma$ if $\gamma \geq n-d$.

The last slide!

$f(X,0) = (X+1)^n$, and for $x_0 \neq 0$ the multi-set $\{\chi_u(x_0) \mid u \in S\}$ contains each p-th root of unity at most $(n-d)$ times, so $f(X,x_0) \mid (X^p+1)^\gamma$ if $\gamma \geq n-d$.

It follows that $h(X,x) := (X^p+1)^\gamma g(X,x)$ is a polynomial of degree $\gamma - n$ for each $x \in G \setminus \{0\}$, finally in the formal power series $h(X,0) = (1+X)^{-n}(1+X^p)^\gamma$ the coefficients of all $X^{>\gamma-n}$ are divisible by p^{k-1} by the characterlemma.