p-ary Weight problems in designs, coding, and cryptography

(preceded by a brief research overview)

Henk Hollmann

Singapore, Nanyang Technological University, 29 Sept. 2010

(mostly joint work with Qing Xiang and others)

Contents

Introduction

Background:
Masters (Association schemes) & Ph.D. (Modulation codes) both from Eindhoven Technical University, the Netherlands, supervisor Jack van Lint (and Paul Siegel)

1982-1985:
CNET (Centre National d'Études des Télécommunications), Issy-les-Moulineaux (Paris), France

Main research:

- FFT (Fast Fourier Transforms) and NTT (Number Theoretic Transforms)
- Hardware design, patent $\longrightarrow$ convolver prototype
- Factorisation of $x^N - q$ over $\mathbb{Q}$.
- Co-inventor (with Pierre Duhamel) of split-radix FFT.

1985-2009:

Philips Research Laboratories, Eindhoven, the Netherlands
(1999-2009: Principal Scientist)

Responsible for Discrete Mathematics within Philips Research

Consultancy and research in Discrete Mathematics, Coding Theory, Cryptography, Information Theory, and Digital Signal Processing.

2010-:

- Eindhoven University of Technology, the Netherlands
- Own math consultancy firm

More “applied” research topics: published on

- Fourier Transforms (FFT, NTT)
- Finite fields (arithmetic)
- Signal processing algorithms (filtering, write-equalization)
- Testing of IC’s (Integrated Circuits)
- Switching networks (self-routing optical switching)
- LFSR’s (Linear Feedback Shift Registers), *m*-sequences
- Block-designs and various design-like stuff
- Optimization, and algorithms [Pascal, Fortran, C, C++, ...]
- Constrained (modulation) codes (Magnetic recording, CD)
- Error-correcting codes, decoding (RS, iterative erasure)
- Video-on-demand
- Cryptography (timing attacks, visual crypto, whitebox crypto)

9 US patents (algorithms, arithmetic, constrained codes, crypto)

More "pure" research topics: published on

- Association schemes
  (schemes related to conic in $\mathrm{PG}(2, q)$, q even, and $\mathrm{PSL}(2, q)$, fusion schemes, finite geometry, Metz/Wilbrink SR graphs, pseudocyclic association schemes)
- Permutation polynomials
- Kloosterman sum identities

- Cryptography - IPP (Codes with Identifiable Parent Property)

- p-rank problems in difference sets, bent functions, sequences

- Coding theory - many topics
  (with Qing Xiang: proof of Welch and Niho conjectures)

Research interests: very broad, with emphasis on

- Algebraic combinatorics
- Finite fields and their applications
- Linear algebra and its applications

I like to collaborate: about 80% of my publications with co-authors

Co-authors include:

Aart Blokhuis, Gary Ebert (Geometry)
Janós Körner, Simon Lytsyn, Jack van Lint [7x] (Combinatorics)
Tor Helleseth, Qing Xiang [13x] (Algebraic combinatorics)

Ludo Tolhuizen [14x] (Coding theory/cryptography/combinatorics)

Pierre Duhamel [7x] (FFT/NTT)
Kees Schouhamer Immink [5x] (constrained coding)

p-Ary weight problems and applications I: Difference sets and their p-ranks

$(G, \cdot)$ abelian group, $|G| = v$.

$D \subseteq G$ is a (v, k, λ)-difference set in G if $|D| = k$ and $\forall a \neq 1_G$ # (d_1, d_2) in D^2 for which

$$d_1 \cdot d_2^{-1} = a$$

equals λ.

$$\left(\sum_{d \in D} d\right)\left(\sum_{d \in D} d^{-1}\right) = (k - \lambda) 1_G + \lambda \sum_{g \in G} g.$$

Consequence:

$$k(k-1) = \lambda(v-1).$$

G cyclic, then D cyclic difference set.

(Complex) character $\chi : (G, \cdot) \mapsto (\mathbb{C}^*, \cdots)$, homomorphism

$\chi_0 : g \mapsto 1 \quad (g \in G)$: trivial character.

Theorem (Character characterization)

Let $|G| = v$, and let k, λ satisfy

$$\lambda(v-1) = k(k-1).$$

Then a k-subset $D \subseteq G$ is (v, k, λ)-difference set iff

$$\chi(D)\overline{\chi(D)} = k - \lambda$$

for every nontrivial ($\neq 1$) complex multiplicative character χ. Here

$$\chi(D) = \sum_{d \in D} \chi(d).$$

Proof by Fourier inversion.

Example

Classical parameters: Singer difference sets.

$$H^* := \{x \in \mathbf{F}_{q^m}^* \mid \mathrm{Tr}(x) = 0\},$$

$$\mathrm{Tr}(x) = \mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x) = x + x^q + \cdots + x^{q^{m-1}}.$$

$\mathrm{Tr}(ax) = a\mathrm{Tr}(x) \quad (a \in \mathbf{F}_q^*)$, so

$$H^* \subset \mathbf{F}_{q^m}^*/\mathbf{F}_q^*.$$

Theorem

H^* is a

$$((q^m-1)/(q-1), (q^{m-1}-1)/(q-1), (q^{m-2}-1)/(q-1))-$$

(cyclic) difference set in $\mathbf{F}_{q^m}^*/\mathbf{F}_q^*$.

Proof?

Gauss and Jacoby sums

$q = p^s$, p prime, $\mathbf{F}_q = \mathrm{GF}(q)$, finite field with q elements,

$\mathbf{F}^* = \mathbf{F} \setminus \{0\}$

$\mathrm{Tr}(x) = \mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p} = x^p + x^{p^2} + \cdots + x^{p^{s-1}}$, trace function.

ξ_n complex n-th root of unity

$$\psi : \mathbf{F}_q \mapsto \mathbb{C}^*, \qquad \psi(x) = \xi_p^{\mathrm{Tr}(x)}$$

is (nontrivial) additive character of $\mathbf{F}_q$

$\chi : \mathbf{F}_q^* \mapsto \mathbb{C}^*$ multiplicative character of $\mathbf{F}_q^*$; define $\chi(0) = 0$.

$\chi^{q-1} = 1$, the trivial character.

Gauss sum

$$g(\chi) = \sum_{a \in \mathbf{F}_q} \chi(a)\psi(a).$$

Elementary property:

$$g(1) = -1, \qquad g(\chi)\overline{g(\chi)} = q, \qquad \chi \neq 1.$$

Note that $g(\chi)$ lives in $\mathbb{Z}[\xi_{q-1}, \xi_p]$.

Jacoby sum

$$J(\chi_1, \chi_2) = \sum_{a \in \mathbf{F}_q} \chi_1(a)\chi_2(1-a).$$

$\chi_1, \chi_2, \chi_1\chi_2 \neq 1$, then

$$J(\chi_1, \chi_2) = g(\chi_1)g(\chi_2)/g(\chi_1\chi_2),$$

and so

$$J(\chi_1, \chi_2)\overline{J(\chi_1, \chi_2)} = q, \qquad \chi \neq 1.$$

Character characterization theorem can be used to prove that D is difference set by expressing $\chi(D)$ in terms of Gauss and Jacoby sums!

Example (Singer) χ non-trivial, then

$$g(\chi) = q\,\chi(H^*),$$

hence $\chi(H^*)\overline{\chi(H^*)} = q^{m-2} = k - \lambda$.

Maschietti difference sets:

$$q = 2^m, \qquad k \text{ integer}, \qquad (k, q-1) = 1.$$

Theorem

If $\tau : x \mapsto x + x^k$ *two-to-one on* $\mathbf{F}_q$ *then* $D_{k,m} = \mathrm{Im}\tau \setminus \{0\}$ *is a* $(2^m - 1, 2^{m-1} - 1, 2^{m-2} - 1)$*-difference set in* $\mathbf{F}_q^*$

Proof: $(k-1, q-1) = 1$, so χ non-trivial, then $\exists \phi : \chi = \phi^{k-1}$; now

$$\chi(D_{k,m}) = \frac{1}{2} J(\phi, \chi) \qquad (\chi = \phi^k).$$

Possible parameters:

- (regular) $k = 2$
- (translation) $k = 2^r$, $(m, r) = 1$, $1 < r < m/2$
- (Segre) $k = 6$
- (Glynn type I) $k = 2^{2r} + 2^r$, $m \geq 7$ odd, $4r \equiv 1 \bmod m$
- (Glynn type II) $k = 3 \cdot 2^r + 4$, $m \geq 11$ odd, $2r \equiv 1 \bmod m$

Nonisomorphic? Compute p-ranks!

p-rank of D is $\mathbf{F}_p$-rank of incidence matrix $A_{g,h} = \delta_{gh^{-1} \in D}$ of associated (symmetric) design.

Only interesting if $p | k - \lambda$ [or $p | k$] (det=0)

- Distinct p-ranks then distinct designs!

p-rank = complexity of associated $0, 1$-sequence char_D.

Theorem
If $\mathrm{char}(\mathbf{F}) \not| v$, $\mathbf{F}$ contains all v^*th roots of 1 ($v^* = \exp(G)$), then p-rank of D equals # $\mathbf{F}$-characters $\chi : G \mapsto \mathbf{F}^*$ with $\chi(D) \neq 0$

Proof: Fourier inversion.

$X_{\chi,g} = \chi(g)$, then $X^{-1}_{g,\chi} = v^{-1}\chi(-g)$, and if $A_{g,h} = \delta_{gh^{-1} \in D}$, then

$$XAX^{-1} = v \cdot \mathrm{diag}(\chi(D))_\chi.$$

Stickelberger's theorem

$q = p^s$, α primitive in $\mathbf{F}_q$, $f(x)$ minimal polynomial of α over $\mathbf{F}_p$

$$\mathfrak{p} = (f(\xi_{q-1}), p)$$

prime ideal in $\mathbb{Z}[\xi_{q-1}]$ lying over p:

$$\mathbb{Z}[\xi_{q-1}]/\mathfrak{p} \cong \mathbf{F}_p[x] \bmod f(x) \cong \mathbf{F}_q,$$

isomorphism:

$$\omega_\mathfrak{p} : \alpha \mapsto \xi_{q-1}$$

$\omega_\mathfrak{p} : \mathbf{F}_q^* \mapsto \mathbb{C}^*$ Teichmüller character.

If $\chi : \mathbf{F}_q^* \mapsto \mathbb{Z}[\xi_v]^* \subset \mathbb{C}^*$ complex multiplicative character, then

$$\chi \bmod \mathfrak{p}$$

multiplicative $\mathbf{F}_q$-character $\mathbf{F}_q^* \mapsto \mathbf{F}_q^*$ $\quad (p = \mathrm{char}(\mathbf{F}_q) \not| |\mathbf{F}_q^*|)$.

Consequence: p-rank of D is # complex characters χ for which

$$\chi(D) \bmod \mathfrak{p} \neq 0.$$

Let

$$\mathfrak{P} = (f(\xi_{q-1}), \xi_p - 1, p)$$

be the prime ideal in $\mathbb{Z}[\xi_{q-1}, \xi_p]$ above $\mathfrak{p}$.

$$(x-1)^{p-1} \equiv x^{p-1} + x^{p-2} + \cdots + x + 1 \bmod p,$$

so $(\xi_p - 1)^{p-1} = 0 \bmod p$ and

$$\mathfrak{P}^{p-1} = \mathfrak{p}, \qquad v_{\mathfrak{P}}(p) = p - 1$$

($v_{\mathfrak{P}}$ is $\mathfrak{P}$-adic valuation).

$q = p^s$, p prime. If

$$a \equiv a_0 + a_1 p + \cdots + a_{p-1} p^{s-1} \neq 0 \bmod q - 1,$$

$0 \leq a_i \leq p-1$, then

$$w(a) = w_p(a) = a_0 + a_1 + \cdots a_{s-1},$$

the p-ary weight of a.

Theorem (Stickelberger)

$$v_{\mathfrak{P}}(g(\omega_{\mathfrak{p}}^{-a})) = w_p(a).$$

So $\mathfrak{P}^{w_p(a)} || g(\omega_{\mathfrak{p}}^{-a})$ and $\mathfrak{p}^{(p-1)w_p(a)} || g(\omega_{\mathfrak{p}}^{-a})$

Example: Singer difference sets, $q = p^s$.

χ character on $\mathbf{F}_{q^m}^*/\mathbf{F}_q^*$;

$\chi = \omega_{\mathfrak{p}}^{-a(q-1)}$, $\quad \chi \neq 1$ iff $(q-1)a \neq 0$ mod $q^m - 1$.

Now

$$g(\omega_{\mathfrak{p}}^{-a(q-1)}) = q \cdot \omega_{\mathfrak{p}}^{-a(q-1)}(H^*),$$

$$v_{\mathfrak{P}}(g(\omega_{\mathfrak{p}}^{-a(q-1)})) = w_p(a(q-1)), \qquad v_{\mathfrak{P}}(q) = (p-1)s,$$

and $\chi_0 = 1$ gives

$$\chi_0(H) = |H^*| \not\equiv 0 \text{ mod } \mathfrak{p}.$$

Conclusion: p-rank $= 1 + \#\, a$, $0 < a < (q^m - 1)/(q-1)$, with

$$w_p((q-1)a) = (p-1)s.$$

Answer: Hadama's formulae ($q = p^s$)

$$1 + \binom{p+m-1}{m-2}^s.$$

Similar, but more complicated, for GMW difference sets (work with Arasu, Player, Xiang)

Example: Maschietti difference sets $D_{k,m}$ in $\mathbf{F}_{2^m}^*$,
$(k, q-1) = (k-1, q-1) = 1$

$$\begin{aligned} \chi(D_{k,m}) &= \frac{1}{2} J(\phi, \chi) \qquad (\chi = \phi^k) \\ &= 2^{-1} g(\chi^{k-1}) g(\chi)/g(\chi^k). \end{aligned}$$

$\chi = \omega_{\mathfrak{p}}^{-a} \longrightarrow$ need # a in $\mathbb{Z}_{2^m-1} \setminus \{0\}$ for which

$$-1 + w_2((k-1)a) + w_2(a) - w_2(ka) = 0.$$

$s, \quad a^{(1)}, \ldots, a^{(k)} \in \mathbb{Z}_{p^m-1}; \quad t_1, t_2, \ldots, t_k \in \mathbb{Z} \setminus \{0\},$

$$s \equiv t_1 a^{(1)} + t_2 a^{(2)} + \cdots + t_k a^{(k)} \bmod p^m - 1.$$

$t_+ = \sum_{i,\ t_i>0} t_i, \quad t_- = \sum_{i,\ t_i<0} t_i.$

Theorem (Molular p-ary add-with-carry algorithm)

$\exists$ *unique* $\gamma = (\gamma_i)_{i \in \mathbb{Z}_m}$, *indices mod m, so* $\gamma_{-1} = \gamma_{m-1}$, *for which*

$$\sum_{j=1}^{k} t_j a_i^{(j)} + \gamma_{i-1} = s_i + p\gamma_i, \quad 0 \le i \le m-1. \tag{1}$$

γ *satisfies*

$$(p-1)w(\gamma) = \sum_{j=0}^{k} t_j w(a^{(j)}) - w(s); \tag{2}$$

$$t_- \le \gamma_i \le t_+ - 1 \tag{3}$$

if $\exists j : a^{(j)} \not\equiv 0 \bmod p^m - 1$.

c_i *modular carries for computation*

Exampe: Segre case $k = 6$

Count a in $\mathbb{Z}_{2^m-1} \setminus \{0\}$ for which

$$w(a) + w(5a) = w(6a) + 1.$$

Method: add-with-carry algorithms. Example: $b = 5a = 4a + a$,

$$a_i + a_{i-2} + \gamma_{i-1} = b_i + 2\gamma_i,$$

indices in $\mathbb{Z}_m$, with $\gamma_i = 0, 1$ for all i.

Similar, $s = 6a = a + b$,

$$a_i + b_i + \delta_{i-1} = s_i + 2\delta_i,$$

indices in $\mathbb{Z}_m$, with $\delta_i = 0, 1$ for all i.

$$[2w(a) = w(b) + w(\gamma)], \qquad w(a) + w(b) = w(s) + w(\delta),$$

so we want $w(a) + w(b) - w(s) = w(\delta) = 1$.

Think of computation as

$$(a_{i-2}, a_{i-1}, \gamma_{i-1}, \delta_{i-1}) \xrightarrow{a_i} (a_{i-1}, a_i, \gamma_i, \delta_i).$$

Labelled digraph: states (vertices) and arcs

$$(a'', a', \gamma', \delta') \longrightarrow (a', a, \gamma, \delta)$$

whenever

$$a'' + a + \gamma' - 2\gamma = b \in \{0,1\}, \qquad a + b + \delta' - 2\delta = s \in \{0,1\},$$

so initial state + a determines b, γ, s, δ, hence terminal state of arc.

V_δ: states (a', a, γ, δ) $\quad (\delta = 0, 1)$

Count B_m= # closed directed paths of length m
starting in $v \in V_1$, through V_0 only, then returning to v.

Counting: tranfer matrix method, $B_m = \mathrm{Tr}(A_{10} A_{00}^{m-2} A_{01})$

$$A_{00} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Minimal polynomial

$$f(X) = X^6 - X^5 - X^4 + X^3 - X^2 + X = X(X-1)(X^4 - X^2 - 1),$$

so

$$A^5 - A^4 - A^3 + A^2 - A + I = O.$$

In fact

$$B_m = B_{m-2} + B_{m-4}.$$

Typically recursive relations for these p-ranks.

Glynn I&II similar but much more complicated, especially Glynn I.

p-Ary weight problems and applications II: Few-weight codes

$q = p^s$, p prime, m, t positive integers, $(t, m) = 1$.

$C_{1,t}$ cyclic code over $\mathbf{F}_q$, length $n = q^m - 1$, defining zero's α, α^t,

α primitive in $\mathbf{F}_{q^m}$. (Usually dimension $k = 2m$.)

$$c = (c_0, c_1, \ldots, c_{n-1}) \in C_{1,t}$$

iff

$$c(\alpha) = c(\alpha^t) = 0,$$

where

$$c(x) = c_0 + c_1 x + \cdots + c_{m-1} x^{m-1} \in \mathbf{F}_q[x] \bmod x^n - 1.$$

$A_0 = 1, A_1, \ldots, A_n$ weights of $C_{1,t}$, where

$$A_w = \{c \in C_{1,t} \mid \mathrm{wt}(c) = w\}.$$

$C_{1,t}^{\perp}$ is dual code, weights $B_0 = 1, B_1, \ldots, B_n$.

Sometimes $C_{1,t}^{\perp}$ few-weight code.

Relation with sequences:

m-sequence $a = a_0, a_1, \ldots, a_{n-1}$: codeword from simplex code $C_1^\perp$.

decimation by a factor t:

$$b = a_0, a_t, a_{2t}, \ldots, a_{nt} \in C_t^\perp.$$

Cross-correlation

$$\theta_{a,b}(\tau) = \sum_{i=0}^{n-1} (-1)^{a_i + b_{i+\tau}} \quad = \quad n - \mathrm{dist}(\mathrm{a}, \mathrm{b}).$$

is weight in $C_{1,t}^\perp$!

Preferred pair of m-sequences: $\theta_{a,b}$ takes only values

$$-1, \quad -1 \pm 2^{\lfloor (m+2)/2 \rfloor};$$

equivalently, non-zero weights in $C_{1,t}^\perp$ are

$$2^{m-1}, \quad 2^{m-1} \pm 2^{\lfloor (m+2)/2 \rfloor - 1}.$$

Not possible if $m \equiv 0 \mod 4$; four known cases with $m \equiv 2 \mod 4$ (character theory proofs for the two difficult ones)

Known cases: with m odd:

- $t = 2^r + 1$, if $(r, m) = 1$ (Gold, 1968)
- $t = 2^{2r} - 2^r + 1$, if $(r, m) = 1$ (Welch, 1969; Kasami, 1971)
- $t = 2^r + 3$, $2r \equiv -1 \mod m$ (conjectured by Welch, 1972)
- $t = 2^{2r} + 2^r - 1$, $4r \equiv -1 \mod m$ (conjectured by Niho, 1972)

More three-weight cases (bigger gaps/CC values) in Gold-Kasami cases with $m/(r, m) = 1$.

Uniform method to prove few-weight results

Step 1: Pless power moment identities

MacWilliams transforms relating weights and dual weights

$$\sum_{w=0}^{n-v} \binom{n-w}{v} B_w = q^{k-v} \sum_{w=0}^{v} \binom{n-w}{v-w} A_w$$

$(v = 0, 1, \ldots, n)$ gives

$$P_i = \sum_{w=1}^{n} w^i B_w = \mathrm{expr}(n, k, A_0, \ldots, A_i)$$

$$0 < w_1 \leq w_2 \leq w_3 \leq w_4 < n,$$

$$E = \sum_{w=1}^{n} (w - w_1)(w - w_2)(w - w_3)(w - w_4) B_w = \mathrm{expr}(n, k, A_3, A_4)$$

$(A_0 = 1, A_1 = A_2 = 0\ )$

$C^{\perp}$ no weights in $(w_1, w_2) \cup (w_3, w_4)$ then

$$E \geq 0,$$

equality iff $C^{\perp}$ has only nonzero weights w_1, w_2, w_1, w_4.

In our case: take $w_2 = w_3 = 2^{m-1}, w_1, w_4 = 2^{m-1} \pm 2^{m-1-M}$

Step 2: Compute low weights of C

Compute A_3, A_4, or show $\min \operatorname{dist}(\mathrm{C}) \geq 5$. Often difficult!

Breakthrough result by Hans Dobbertin:
both Welch and Niho codes have minimum distance 5.

If few-weight assumption correct, then now $E = 0$.

Step 3:

Find restrictions on weights of $C = C_{1,t}^{\perp}$: McEliece's lemma

Theorem (McEliece)

C binary cyclic code, B_w weight enumerator, ℓ smallest positive number for which ℓ nonzero's of C (repetitions allowed, not all 1) have product 1. Then

$$2^{\ell-1} | B_w \qquad (w > 0), \qquad \exists w : 2^{\ell} \not| B_w.$$

Some proof method involve Gauss-sums and Stickelberger's theorem!

Example: $C = C_{1,t}^{\perp}$. Now $C^{\perp} = C_{1,t}$ has zero's α^i for i one of

$$1, 2, 4, \ldots, 2^{m-1}; \qquad t, 2t, 4t, \ldots, 2^{m-1}t.$$

nonzero's of $C = C_{1,t}^{\perp}$ are (Fourier inversion) α^j for j one of

$$\begin{array}{cc} -1, -2, -4, \ldots, -2^{m-1}; & -t, -2t, -4t, \ldots, -2^{m-1}t. \\ \bigvee & \bigvee \\ b & a \end{array}$$

product is 1 iff

$$-b - ta \equiv 0 \bmod 2^m - 1, \qquad \bar{b} \equiv ta \bmod 2^m - 1;$$

$\#$ is $w(b) + w(a) = m - w(\bar{b}) + w(a) = m - (w(ta) - w(a)$

$$\ell = m - M(m;t), \qquad M(m;t) = \max_{a \in \mathbb{Z}_{2^m-1} \setminus \{0\}} \Big(w(ta) - w(a) \Big).$$

Gold case:

$$M(m;2^r+1) = \begin{cases} m/2, & m/(r,m) \text{ even;} \\ (m-(r,m))/2, & m/(r,m) \text{ odd.} \end{cases}$$

Proof:

$$M(m;2^r+1) = \max_{a\in\mathbb{Z}_{2^m-1}\setminus\{0\}} \Big(w((2^r+1)a) - w(a) \Big).$$

$s = (2^r+1)a = 2^r a + a$,

$$a_i + a_{i-r} + \gamma_{i-1} = s_i + 2\gamma_i, \qquad i \in \mathbb{Z}_m,$$

with $\gamma_i = 0, 1$.

$2w(a) = w(s) + w(\gamma)$. Put $\omega = a_i - \gamma_i \implies$
$w(s) - w(a) = w(\omega)$.

$$\omega_i = 1 \implies a_i = 1, \gamma_i = 0 \implies a_{i-r} = 0 \implies \omega_{i-r} \leq 0.$$

Partition $\omega_0, \ldots, \omega_{m-1}$ into groups

$$(\omega_i, \omega_{i-r}, \ldots, \omega_{i+r}).$$

\# groups $e = (r, m)$, each size $L = m/(r, m)$.

Weight per group $\leq \lfloor L/2 \rfloor$

$\square$

Kasami case similar.

Welch and especially Niho cases much more complicated!

Niho digraph (after trick) has 1296 vertices.

p-Ary weight problem III: Algebraic immunity

Boolean functions on m variables:

$$f : \mathbf{F}_{2^m} \mapsto \mathbf{F}_2, \qquad f = \sum_{a \in \mathbb{Z}_{2^m-1}} f_a x^a,$$

$$x^a = x_0^{a_0} x_1^{a_1} \cdots x_{m-1}^{a_{m-1}}, \qquad \deg(x^a) = w(a),$$

$$a = a_0 + a_1 2 + \cdots + a_{m-1} 2^{m-1}.$$

Algebraic immunity

$$AI_m(f) = \min\{\deg(g) \mid g \neq 0, \;\; f \cdot g = 0 \text{ or } (f+1) \cdot g = 0\}.$$

$AI_m(f) \leq \lfloor \frac{m}{2} \rfloor$ (Courtois)

α primitive in $\mathbf{F}_{2^m}$.

$$\Delta = \{\alpha^0 = 1, \alpha, \alpha^2, \ldots, \alpha^{2^{m-1}}\},$$

Define

$$g : \mathbf{F}_{2^m} \mapsto \mathbf{F}_2, \qquad \mathrm{supp}(g) = \Delta;$$

$$f : \mathbf{F}_{2^m} \times \mathbf{F}_{2^m} \mapsto \mathbf{F}_2, \qquad f(x,y) = g(xy^{2^m-2}).$$

$$\Psi = \mathrm{supp}(f) = \{(\gamma y, y) \mid \gamma \in \Delta,\ y \in \mathbf{F}_{2^m}^*\}$$

f is bent (Dillon)

Conjecture (Tu, Deng)

$AI_{2m}(f) = m$, maximal.

Conjecture (Tu, Deng)

$h(x,y)=\sum_{a,b\in\mathbb{Z}_{2^m-1}} h_{a,b}x^a y^b$ zero on Ψ, then $\deg(h)\geq m$*.*

If not, then

$$h_{a,b}=0, \qquad w(a)+w(b)\geq m.$$

$$\sum_{\substack{a,b\in\mathbb{Z}\\ a+b=s}} h_{a,b}\gamma^a = 0 \qquad (\gamma\in\Delta)$$

for all $s\in\mathbb{Z}_{2^m-1}\setminus\{0\}$.

$h^{(s)}=(h_{0,s},h_{1,s-1},\ldots,h_{s,0},h_{s+1,2^m-2},\ldots,h_{2^m-2,s+1})\in \mathrm{BCH}(\Delta)$,

so 0, or weight $\geq 2^{m-1}+1$.

Conjecture (Tu,Deng)

$\#\,(a,b)$ with $a,b\in\mathbb{Z}_{2^m-1}\setminus\{0\}$ and $a+b\equiv s$ for which

$$w(a)+w(b)\leq m-1$$

is at most 2^{m-1}.

Almost solved using modular 2-ary add-with-carry techniques

Conclusions

- weight (in)equalities mostly derived by deep and powerful algebraic methods (character theory, p-adic methods, ...)
- Leads to interesting mathematics.
- p-Ary weight techniques are a valuable tool in algebraic combinatorics.