Low Rank Relative Difference Sets Using Galois Rings

Qing Xiang† and Jim Davis‡

†Supported by NSA grant MDA 904-99-1-0012

‡Supported by a grant from Hewlett-Packard

Definition 1 *A Relative Difference set (RDS) in a group G of order mu relative to a normal subgroup U of order u is a subset D with k elements so that every element of $G \backslash U$ is represented exactly λ times as $d_1 d_2^{-1}$.*

Example 2 $G = \langle x, y | x^4 = y^2 = 1 \rangle, U = \langle x^2 \rangle$: $D = \{1, y, x, x^3 y\}$ *is a* $(m, u, k, \lambda) = (4, 2, 4, 2)$ *RDS.*

- Parameters for this talk: $(m, u, k, \lambda) = (2^{2t}, 2^t, 2^{2t}, 2^t)$
- Previously known: any abelian group, rank $\geq 2t \ldots$

WITH ONE EXCEPTION!!

Arasu-Sehgal example:

Example 3 $G = \langle x, y, z | x^4 = y^4 = z^4 = 1\rangle, U = \langle x^2, y^2\rangle, D = B_1 \cup zB_2$ *is a (16,4,16,4) RDS for* $B_i \subset \langle x, y, z^2\rangle$.

Ray-Chaudhuri, Xiang view: Use Galois Rings.

$GR(4,2) = Z_4[X]/\langle X^2 + X + 1\rangle, X^3 = 1.$

$F_0 = \mathcal{T} = \{0, 1, X, X^2\}$
$(= \{1, x, y, x^3y^3\})$

$B_1 = (F_0, 1) \cup ((1 + 2)F_0, z^2)$
$(= \{1, x, y, x^3y^3, z^2, x^3z^2, y^3z^2, xyz^2\})$

$V = \{0, 2\}; \alpha_1 = 0, \alpha_2 = 2X$

$B_1 = ((1 + 0 + 0)F_0, 0) \cup ((1 + 0 + 2)F_0, 2);$
$B_2 = ((1 + 2X + 0)F_0, 0) \cup ((1 + 2X + 2)F_0, 2)$

Example 4 *(New construction) Consider* $GR(4,3) = Z_4[X]/\langle X^3+2X^2+X+3\rangle, X^7 = 1.$

$V = \{0, 2, 2X, 2X+2\}; \alpha_1 = 0, \alpha_2 = 2X^2$

$B_1 = ((1+0+0)F_0, 0) \cup ((1+0+2)F_0, 2) \cup (1+0+2X)F_0, 2X) \cup ((1+0+2X+2)F_0, 2X+2);$

$B_2 = ((1+2X^2+0)F_0, 0) \cup ((1+2X^2+2)F_0, 2) \cup (1+2X^2+2X)F_0, 2X) \cup ((1+2X^2+2X+2)F_0, 2X+2)$

Key idea: Find a V as small as possible so that the B_i have good character theoretic properties.

Hou's idea: Find the dual of V under an appropriate inner product.

Definition 5 *Define* $s(2,t) = max_{a \in 1+2\mathcal{T}}\{dim W \mid$ W *is a* $GF(2)$*-subspace of* $R/2R$ *and* $W \subseteq \{\pi(x) \in R/2R \mid T(ax) = 0, x \in \mathcal{T}\}\}$

For our purposes, $V = W^{\perp}$. Thus, the problem boils down to computing $s(2,t)$. Reading $T(ax)$ 2-adically, we get

$$T(ax) = b_x + 2c_x$$

where $b_x = tr(\overline{x})$ and $c_x = Q(\overline{x}) + tr(\eta\overline{x}), Q(\overline{x}) = \sum_{0 \le i < j \le t-1} \overline{x}^{2^i+2^j}$ and η an element of the finite field associated to a.

Quadratic forms to the rescue

After some computations (including using Hilbert's Theorem 90), we see that the quadratic form $Q_{\mathcal{R}}(y) = tr(y\mathcal{R}(y)) = tr(y((\eta^2+\eta+1)y+y^2))$ will be very useful.

After computing the radical of $Q_{\mathcal{R}}(y)$ and observing odd/even possibilities, we get the following theorem:

Theorem 6 $s(2,t) = \lfloor \frac{t}{2} \rfloor$

Idea of proof: We can choose η so that the quadratic form is hyperbolic. The Witt Index implies that the maximal vanishing subspace of the quadratic form has the appropriate size. We tinker with a few details to get the result.

Consequences of knowing $s(2,t)$

Theorem 7 *If* $|G| = 2^{3t}$ *and* G *contains a subgroup isomorphic to* $Z_4^t \times Z_2^{\lceil \frac{t}{2} \rceil}$, *then* G *has a* $(2^{2t}, 2^t, 2^{2t}, 2^t)$ *RDS relative to the appropriate subgroup.*

Partial Difference Set (PDS) implications: pins down the possible parameters for a certain type of Latin Square PDS. This was Hou's (and Ray-Chaudhuri–Xiang's) original motivation for studying this problem.

Open Questions

1. Is there an analogous result for $s(p,t)$ for p odd?

2. Connections to McFarland Difference Sets?

3. Can we lower the rank any further?

4. Can we use this to say anything regarding $(2^{2a}, 2^b, 2^{2a}, 2^{2a-b})$ for $b > a$?