Twisted symplectic polar graphs and Gordon-Mills-Welch difference sets

Akihiro Munemasa\(^1\)
(joint work with Frédéric Vanhove)

\(^1\)Graduate School of Information Sciences
Tohoku University

February 28, 2014
Colloquium on Galois Geometry
to the memory of
Frédéric Vanhove (1984-2013)
Ghent University
The symplectic polar graph associated with the group $\text{Sp}(2n, 2)$:

$$X = V(2n, 2) - \{0\}$$

$u \sim v \iff$ orthogonal

$\text{SRG}(2^{2n} - 1, 2^{2n-1} - 1, 2^{2n-2} - 3, 2^{2n-2} - 1)$. 

Another description:

$V = V(2, 2^n)$, $f : V \times V \to \text{GF}(2^n)$: a nondegenerate alternating form.

$$X = V - \{0\}$$

$u \sim v \iff \text{Tr} \ f(u, v) = 0$. 

SRG($2^{2n} - 1, 2^{2n-1} - 1, 2^{2n-2} - 3, 2^{2n-2} - 1$).

There is a graph having these parameters but not isomorphic to the symplectic polar graph.

$W = V(3, 2^n)$, $Q : W \rightarrow \mathbb{GF}(2^n)$: a nondegenerate quadratic form.

$$X = \{ \langle x \rangle \mid x \in W, \ Q(x) \neq 0, \ \langle x \rangle \neq W^\perp \},$$

$\langle x \rangle \sim \langle y \rangle \iff \langle x, y \rangle$: secant or tangent.

In both graphs, there are two kinds of edges.
Note that, in $\text{Sp}(2n, 2)$-graph, given $0 \neq u \in V(2, 2^n)$,

\[
|\{v \in V(2, 2^n) \mid v \neq 0, v \neq u, f(u, v) = 0\}| = 2^n - 2,
|\{v \in V(2, 2^n) \mid f(u, v) \neq 0, \text{Tr} f(u, v) = 0\}| = 2^{2n-1} - 2^n.
\]

In $O(3, 2^n)$-graph, given a point $\langle x \rangle \in X$,

\[
|\{\langle y \rangle \in X \mid \langle x, y \rangle \text{ tangent}\}| = 2^n - 2,
|\{\langle y \rangle \in X \mid \langle x, y \rangle \text{ secant}\}| = 2^{2n-1} - 2^n.
\]

$Q \to$ alternating form $f$ on $\overline{W} = W/W^\perp$.

Given $\langle x \rangle, \langle y \rangle \in X$ with $Q(x) = Q(y) = 1$,

\[
Q(\alpha x + \beta y) = \alpha^2 + f(\bar{x}, \bar{y})\alpha\beta + \beta^2.
\]

$\exists t \in \text{GF}(2^n), t^2 + bt + 1 = 0 \iff b = 0$ or $\text{Tr} b^{-1} = 0$

$\exists t \in \text{GF}(2^n), t^2 + t + b = 0 \iff \text{Tr} b = 0$ So $\langle x, y \rangle$
tangent or secant if and only if

\[
\text{Tr} f(\bar{x}, \bar{y})^{2^n-2} = 0 \quad \text{(not } \text{Tr} f(\bar{x}, \bar{y}) = 0)\]

$V = V(2, 2^n)$, $f : V \times V \to \text{GF}(2^n)$: alternating. Fix a positive integer $i$ with $(i, 2^n - 1) = 1$.

$$X = V - \{0\},$$

$$x \sim y \iff \text{Tr}(f(x, y)^i) = 0.$$

Then $\text{SRG}(2^{2n} - 1, 2^{2n-1} - 1, 2^{2n-2} - 3, 2^{2n-2} - 1)$.

$i = 1$: ordinary symplectic polar graph

$i = -1$: graph obtained from $O(3, 2^n)$.

**BCN**=Brouwer-Cohen-Neumaier, Distance-Regular Graphs, 1989

**BCN** gives a 3-class association scheme based on $O(3, 2^n)$. Relations are ‘secant’, ‘external’, ‘tangent’. $\text{secant} \cup \text{tangent}$ gives a SRG.
\[ X = \{ \text{external points}, \neq \text{nucleus} \} \text{ in } O(3, 2^n)-\text{space.} \]

\[ R_1 = \{ (\langle x \rangle, \langle y \rangle) \mid \langle x, y \rangle \text{ secant} \}, \]
\[ R_2 = \{ (\langle x \rangle, \langle y \rangle) \mid \langle x, y \rangle \text{ external} \}, \]
\[ R_3 = \{ (\langle x \rangle, \langle y \rangle) \mid \langle x, y \rangle \text{ tangent} \}. \]

BCN: these relations define an association scheme.

Since there is no group having \( R_i \)'s as orbitals, the proof has to be a geometric one. One needs to show that

\[ p_{ij}^k = |\{ \langle z \rangle \mid (\langle x \rangle, \langle z \rangle) \in R_i, (\langle z \rangle, \langle y \rangle) \in R_j \}| \]

depends only on \( k \) and is independent of \( (\langle x \rangle, \langle y \rangle) \in R_k \).
The reason why I was interested in this association scheme was:

Ikuta and I found a family of complex Hadamard matrices, this was one of the few in E. van Dam’s list (1999) of 3-class association schemes which admits complex Hadamard matrices.

I wanted make sure that

- these association schemes exist,
- extend our results to obvious larger family.

\( O(3, 2^n) \implies O(2n + 1, 2^n) \).

BCN went on to claim \( \exists \) 3-class association scheme for \( O(2m + 1, 2^n) \) without proof, without \( p_{ij}^h \).
BCN went on to claim \( \exists \) 3-class association scheme:
\[ W = V(2m + 1, q) \] with quadratic form,
\[
X = \{ \text{external points, } \neq \text{nucleus} \},
\]
\[
R_1 = \{ (\langle x \rangle, \langle y \rangle) \mid \langle x, y \rangle \text{ secant} \},
\]
\[
R_2 = \{ (\langle x \rangle, \langle y \rangle) \mid \langle x, y \rangle \text{ external} \},
\]
\[
R_3 = \{ (\langle x \rangle, \langle y \rangle) \mid \langle x, y \rangle \text{ tangent} \}.
\]

Frédéric Vanhove: this is incorrect for \( m > 1 \).

\[
R_3 = \{ (\langle x \rangle, \langle y \rangle) \mid \text{nucleus } \in \langle x, y \rangle \text{ tangent} \},
\]
\[
R_4 = \{ (\langle x \rangle, \langle y \rangle) \mid \text{nucleus } \notin \langle x, y \rangle \text{ tangent} \},
\]

If \( m = 1 \), then \( R_4 = \emptyset \). \( R_1 \cup R_3 \cup R_4 \): SRG.
BCN went on to claim \( \exists \) 3-class association scheme: \( W = V(2m + 1, q) \) with quadratic form,

\[
X = \{ \text{external points, } \neq \text{nucleus} \}, \\
R_1 = \{ (\langle x \rangle, \langle y \rangle) \mid \langle x, y \rangle \text{ secant} \}, \\
R_2 = \{ (\langle x \rangle, \langle y \rangle) \mid \langle x, y \rangle \text{ external} \}, \\
R_3 = \{ (\langle x \rangle, \langle y \rangle) \mid \langle x, y \rangle \text{ tangent} \}.
\]

Frédéric Vanhove: this is incorrect for \( m > 1 \).

\[
R_3 = \{ (\langle x \rangle, \langle y \rangle) \mid \text{nucleus } \in \langle x, y \rangle \text{ tangent} \}, \\
R_4 = \{ (\langle x \rangle, \langle y \rangle) \mid \text{nucleus } \notin \langle x, y \rangle \text{ tangent} \},
\]

If \( m = 1 \), then \( R_4 = \emptyset \). \( R_1 \cup R_3 \cup R_4 : \text{SRG} \).

It admits ‘twisted’ symplectic description.
\(V = V(2m, 2^n), f : V \times V \to \text{GF}(2^n)\): alternating. Fix a positive integer \(i\) with \((i, 2^n - 1) = 1\).

\[
X = V - \{0\},
\]

\[
u \sim v \iff \text{Tr}(f(u, v)^i) = 0.
\]

Then SRG\((2^{2mn} - 1, 2^{2mn-1} - 1, 2^{2mn-2} - 3, 2^{2mn-2} - 1)\).

\(i = 1\): ordinary symplectic polar graph

\(i = -1\): graph obtained from \(O(2m + 1, 2^n)\).

\[
R_1 = \{(u, v) \mid f(u, v) \neq 0, \text{Tr}(f(u, v)^i) = 0\},
\]

\[
R_2 = \{(u, v) \mid \text{Tr}(f(u, v)^i) = 1\},
\]

\[
R_3 = \{(u, v) \mid \langle u \rangle_{\text{GF}(2^n)} = \langle v \rangle_{\text{GF}(2^n)}\},
\]

\[
R_4 = \{(u, v) \mid f(u, v) = 0, \langle u \rangle_{\text{GF}(2^n)} \neq \langle v \rangle_{\text{GF}(2^n)}\}.
\]
SRG($2^{2mn} - 1, 2^{2mn-1} - 1, 2^{2mn-2} - 3, 2^{2mn-2} - 1$)

$\lambda + 2 = \mu$

3- or 4-class association scheme $\xrightarrow{\text{secant} \cup \text{tangent}}$ SRG

GMW difference set $\xrightarrow{}$ Hadamard design

(Bill Kantor, Nov. 16, 2013)
\[ V = V(2m, 2^n), \ f: \text{alternating form on } V. \]

\[ R_1 = \{(x, y) \mid f(x, y) \neq 0, \ \text{Tr } f(x, y) = 0\}, \]
\[ R_2 = \{(x, y) \mid \text{Tr } f(x, y) \neq 0\}, \]
\[ R_3 = \{(x, y) \mid \langle x \rangle_{\text{GF}(2^n)} = \langle y \rangle_{\text{GF}(2^n)}\}, \]
\[ R_4 = \{(x, y) \mid f(x, y) = 0, \ \langle x \rangle_{\text{GF}(2^n)} \neq \langle y \rangle_{\text{GF}(2^n)}\}. \]

\[ D = \text{Tr}^{-1}(0) - \{0\} \subset \text{GF}(2^n)^\times: \text{difference set.} \]

\[ R_1 \cup R_3 \cup R_4 = \{(x, y) \mid x \neq y, \ f(x, y) \in D \cup \{0\}\}. \]

Gordon-Mills-Welch (1969): \( R_1 \cup R_3 \cup R_4: \text{SRG.} \)

Its isomorphism type depends on the choice of \( D \).

If \( D = \text{Tr}^{-1}(0) - \{0\} \subset \text{GF}(2^n)^\times \): difference set, then 
\( \mu_i(D) = \{ \alpha^i \mid \alpha \in D \} \) is also a difference set if 
\( (i, 2^n - 1) = 1 \) (equivalent).

SRG from \( D \) has edges \( \{(x, y) \mid f(x, y) \in D \cup \{0\}\} \), 
SRG from \( \mu_i(D) \) has edges \( \{(x, y) \mid f(x, y) \in \mu_i(D) \cup \{0\}\} \).


\[
\text{SRG from } D \cong \text{SRG from } \mu_i(D) \\
\iff i \text{ is a power of } 2 \text{ modulo } 2^n - 1.
\]

In particular for \( i = -1 \), one obtains non-isomorphic SRG.
More generally, Gordon–Mills–Welch (GMW) difference set Ingredients:

- $q$: prime power
- $n \geq 2$
- $D$: difference set whose development is a design with the same parameters as $\text{PG}(n-1, q)$
- $k \geq 2$

Output: difference set whose development is a design with the same parameters as $\text{PG}(kn - 1, q)$

Isomorphism determined by Jackson-Wild, Kantor.
Setting $k = 2m$, we have ...
$D \subset \text{PG}(n - 1, q) = \text{GF}(q^n)^\times / \text{GF}(q)^\times$ a difference set with parameters

$\left( \frac{q^n - 1}{q - 1}, \frac{q^{n-1} - 1}{q - 1}, \frac{q^{n-2} - 1}{q - 1} \right)$,

$\tilde{D} \subset \text{GF}(q^n)^\times$ denote the preimage of $D$.

$X$ the points of $\text{PG}(2mn - 1, q)$ based on the vector space $V = V(2m, q^n)$, regarded as a vector space over $\text{GF}(q)$.

$f : V \times V \to \text{GF}(q^n)$: alternating.

Since $\tilde{D}$ is invariant under $\text{GF}(q)^\times$, for $[x], [y] \in X$, the condition $f(x, y) \in \tilde{D}$ and $f(x, y) = 0$ are independent of the choice of representatives.
\( X \): the points of \( \text{PG}(2mn - 1, q) \) based on the vector space \( V = V(2m, q^n) \), regarded as a vector space over \( \text{GF}(q) \).

\[
R_0 = \{ ([x], [x]) \mid [x] \in X \},
\]
\[
R_1 = \{ ([x], [y]) \mid [x], [y] \in X, f(x, y) \in \tilde{D} \},
\]
\[
R_2 = \{ ([x], [y]) \mid [x], [y] \in X, f(x, y) \neq 0, f(x, y) \notin \tilde{D} \},
\]
\[
R_3 = \{ ([x], [y]) \mid [x], [y] \in X, \langle x \rangle_{\text{GF}(q^n)} = \langle y \rangle_{\text{GF}(q^n)} \},
\]
\[
R_4 = \{ ([x], [y]) \mid [x], [y] \in X, f(x, y) = 0, \langle x \rangle_{\text{GF}(q^n)} \neq \langle y \rangle_{\text{GF}(q^n)} \}.
\]

Note that, if \( m = 1 \), then \( V = V(2, q^n) \), so

\[
f(x, y) = 0 \iff \langle x \rangle_{\text{GF}(q^n)} = \langle y \rangle_{\text{GF}(q^n)}.
\]

Thus \( R_4 = \emptyset \).
Theorem

\( X \): the points of \( \text{PG}(2mn - 1, q) \) based on the vector space \( V = V(2m, q^n) \), regarded as a vector space over \( \text{GF}(q) \).

\[ R_0 = \{ ([x], [x]) \mid [x] \in X \}, \]
\[ R_1 = \{ ([x], [y]) \mid [x], [y] \in X, \ f(x, y) \in \tilde{D} \}, \]
\[ R_2 = \{ ([x], [y]) \mid [x], [y] \in X, \ f(x, y) \neq 0, \ f(x, y) \notin \tilde{D} \}, \]
\[ R_3 = \{ ([x], [y]) \mid [x], [y] \in X, \ \langle x \rangle_{\text{GF}(q^n)} = \langle y \rangle_{\text{GF}(q^n)} \}, \]
\[ R_4 = \{ ([x], [y]) \mid [x], [y] \in X, \ f(x, y) = 0, \ \langle x \rangle_{\text{GF}(q^n)} \neq \langle y \rangle_{\text{GF}(q^n)} \}. \]

\((X, \{ R_i \}_{i=0}^4)\) is an association scheme.

In particular, one obtains a 3-class association scheme from \( O(3, 2^n) \).