GENERALIZED RELATIVE DIFFERENCE SETS

STANLEY E. PAYNE

Abstract. A Bruck-Ryser type nonexistence theorem is given for a class of generalized relative difference sets. Some well-known results on \((v, k, \lambda)\)-designs are generalized and a new class of relative difference sets is given.

1. A Bruck-Ryser type nonexistence theorem. Let \(m\) and \(n\) be positive integers with \(m > 1\). Let \(P_0\) be the identity matrix \(I_{mn}\) of order \(mn\); \(P_1\) the matrix \(J_{mn}\) of order \(mn\) each entry of which is \(1\); \(P_2\) the direct sum of \(J_n\) taken \(m\) times, where \(J_n\) is the matrix of order \(n\) each entry of which is \(1\). Then \(P_0, P_1, \text{ and } P_2\) form a basis for a commutative, linear associative algebra \(A^*\) over the rationals \(Q\). Let \(B = \sum_{i=0}^{2} c_i P_i\), where \(c_i \in Q\). Then put

\[
\begin{align*}
\theta_0 &= c_0 + mn c_1 + nc_2, \\
\theta_1 &= c_0 + nc_2, \\
\theta_2 &= c_0.
\end{align*}
\]

If \(f(x) = \sum_{i=0}^{2} (x - \theta_i)\), a straightforward computation shows that \(f(B) = 0\). Furthermore, \(\theta_i\) (formally) has multiplicity \(k_i\) as a characteristic root of \(B\) where \(k_0 = 1, k_1 = m - 1, k_2 = m(n - 1)\). Let \(W_i\) be the space of characteristic (column) vectors of \(B\) associated with \(\theta_i\), \(i = 0, 1, 2\). Then as in [7] a basis for \(W_i\) has discriminant \(q_i\) relative to the standard Euclidean inner product, where \(q_0 = mn, q_1 = mn, q_2 = n^m\).

Let \(A\) be a rational matrix such that \(A' A = B\). Thus if \(w_1, w_2\) are vectors in \(W_i\), \((A w_1 | A w_2) = (A' A w_1 | w_2) = \theta_i (w_1 | w_2)\), where \((\cdot | \cdot)\) denotes the standard inner product. Then if \(W_i\) is invariant under \(A\), which it will be if \(A\) is normal, in the terminology of Goldhaber [3] \(A\) induces a similarity transformation of norm \(\theta_i\) on \(W_i\) relative to \((\cdot | \cdot)\) restricted to \(W_i\). Applying Goldhaber's theorem we have the following:

**Lemma 1.1.** If \((\cdot, \cdot)_p\) denotes the Hilbert symbol, then

Presented to the Society, January 25, 1969, under the title A generalized incidence equation; received by the editors July 1, 1969.

AMS Subject Classifications. Primary 0520; Secondary 1005, 1010, 2025, 5080.

Key Words and Phrases. Bruck-Ryser, relative difference set, incidence matrix, Hilbert symbol.

1 This research was supported in part by a Miami University Summer (1969) Research Grant.
for all primes $p$, $i = 0, 1, 2$, if $A$ is normal.

From here on assume that the $c_i$'s have been chosen so that
to that $A$ is a $(0, 1)$-matrix. Thus $f(x)$ is the minimal polynomial for $B = A'A$ and $A$ is invertible.

Lemma 1.2. Set $J = J_{mn}$. Then $JA = AJ = (c_0 + c_1 + c_2)J$, and
$\theta_0 = c_0 + mnc_1 + nc_2 = (c_0 + c_1 + c_2)^2$, so that Lemma 1.1 says nothing if

Proof. $A'A = c_0 I + c_1 J + c_2 (I_m \otimes J_n)$ implies $JA = (c_0 + c_1 + c_2)J$.
Then $0 \neq J = (JA)A^{-1}$ implies $c_0 + c_1 + c_2 \neq 0$ and $(c_0 + c_1 + c_2)^{-1}J = JA^{-1}$.
And $JA' = JB = \theta_0 J$ implies $JA' = \theta_0 (c_0 + c_1 + c_2)^{-1}J = AJ$, and $J(AJ) = \theta_0 (c_0 + c_1 + c_2)^{-1}mnJ$.
But $(JA)J = (c_0 + c_1 + c_2)^2 J$, implying $\theta_0 = (c_0 + c_1 + c_2)^2$ as claimed.

Lemma 1.3. Consider $A$ as a matrix of $n \times n$ blocks $A_{ij}$, $1 \leq i, j \leq m$.
Then $A$ is normal if and only if $J_n A_{ij} = A_{ij} J_n$.

Proof. $AA' = A'(A'A)A^{-1} = A^{-1}BA = c_0 I + c_1 J + c_2 [A^{-1}(I_m \otimes J_n)A]$.
So $A$ is normal if and only if $A(I_m \otimes J_n) = (I_m \otimes J_n)A$. Since the $(i, j)$
block of $A(I_m \otimes J_n)$ is $A_{ij} J_n$ and that of $(I_m \otimes J_n)A$ is $J_n A_{ij}$, the
lemma follows.

Assume in addition that $A$ is a $(0, 1)$-matrix with $c_2 = -c_1$, $c_0 > 0$.
$A$ then has row and column sums equal to $c_0$; $c_1$ is positive; and
$\theta_0 = c_0^2$. Equating the $(i, j)$ blocks on each side of the equation $A'A = c_0 I + c_1 J + c_2 (I_m \otimes J_n)$, we have
$\sum_{k=1}^{m} (A_{ik})'A_{kj} = \delta_{ij} c_0 I_n + [c_1 + \delta_{ij} c_2] J_n = \delta_{ij} c_0 I_n + (1 - \delta_{ij}) c_1 J_n$. Putting $i = j$ in this equation we see that the
columns of a given block $A_{ki}$ must be orthogonal. Since $A$ is a $(0, 1)$-
matrix, by Lemma 1.3 $A$ is normal if and only if each $A_{ij}$ is either 0
or a permutation matrix.

Suppose there exists a normal $(0, 1)$-matrix $A$ with three distinct
nonzero characteristic roots such that $A'A = c_0 I + c_1 J - c_1 (I_m \otimes J_n)$.
Here $c_0$, $c_1$, $m$, $n$ are positive integers with $m > 1$, and in general, we
continue to use the notation developed above. In particular, this
means that for each $i$, $1 \leq i \leq m$, there are $c_0$ $k$'s such that $A_{ik}$ is an
$n \times n$ permutation matrix. For the other $k$'s, $A_{ik} = 0$. From the existence
of such an $A$ we may conclude the following lemma and two
theorems.

Lemma 1.4. If $m$ is odd, $n$ even, then $c_0$ is a square. If $m$ is even, then
$c_0 - nc_1$ is a square. And in any case $c_0^2 = c_0 + nc_1 (m - 1)$.

Proof. We have
\[ \det(A'A) = (\det A)^2 = \theta_1 \theta_2^{m-1} \theta_3^{n-1} = c_0(c_0 - nc_1)^{m-1} c_0^{m(n-1)}, \]

using Lemma 1.2.

The restrictions of Lemma 1.1 become in this case:

**Theorem 1.5.** For all primes \( p \):

(i) If \( m \) is odd, then \( (c_0 - nc_1, ( -1)^{\frac{m-1}{2} mn})_p = +1 \),

(ii) If \( m \) and \( n \) are odd, then \( (c_0, ( -1)^{\frac{n-1}{2} n})_p = +1 \),

(iii) If \( m \equiv 2 \pmod{4} \) and \( n \) is even, then \( (c_0, -1)_p = +1 \).

If \( n = 1 \), then \( A \) is the incidence matrix of a \( (v, k, \lambda) \)-design with \( v = m, k = c_0, \) and \( \lambda = c_1 \). And the results of this section become well-known results for such designs.

If \( n \geq 1 \), we say that a design for which \( A \) is an incidence matrix is a relative design \( D(m, n, c_0, c_1) \), since it generalizes the notion of relative difference set \([2]\). The following theorem contains Corollary 2.1.2 of \([2]\).

**Theorem 1.6.** Let \( A^* \) be the \( m \times m \) matrix obtained by replacing the \((i, j)\) block \( A_{ij} \) of \( A \) by a 1 if \( A_{ij} \neq 0 \), and by 0 otherwise. Then \((A^*)'A^* = (c_0 - nc_1)I_m + nc_1J_m \), so that \( A^* \) is the incidence matrix of a \( (v, k, \lambda) \)-design with \( v = m, k = c_0, \lambda = nc_1 \).

**Proof.** This is essentially the content of the remarks following Lemma 1.3.

The Bruck-Ryser-Chowla theorem applied to \( A^* \) says that if \( m \) is odd, then \( (c_0 - nc_1, ( -1)^{\frac{m-1}{2} n}c_1)_p = +1 \) for all primes \( p \). We ask: Just when is this equivalent (at least for relative designs) to the first part of Theorem 1.5? For example, suppose \( m = \frac{1}{2}(2 + s + s^2), \) \( n = 2, \) \( c_0 = 1 + s, c_1 = 1 \). This is the case in which \( A \) is the incidence matrix of a \( v \times v \) \( (3, s, s) \)-configuration \([8]\) with \( v = 2 + s + s^2 \), which is the case covered by the announcement \([6]\). If \( m \) is odd, then by Lemma 1.4 we know \( s + 1 \) is a square. By considering the three cases \( s \equiv 0, 3, 7 \pmod{8} \) and using the fact that \( s + 1 \) is a square, we can show that both the Bruck-Ryser-Chowla theorem \([9]\) applied to \( A^* \) and the first part of Theorem 1.5 are equivalent in this case to the following: if \( s \equiv 3 \pmod{8} \) and if \( p \) is a prime dividing the square free part of \( s - 1 \), then \( p \equiv 7 \pmod{8} \).

2. **Examples.** A set \( R \) of \( c_0 \) elements in a group \( G \) of order \( mn \) is a difference set of \( G \) relative to a normal subgroup \( H \) of order \( n \neq mn \) if the collection of differences \( r - s; r, s \in R, r \neq s \), contains only the elements of \( G \) which are not in \( H \), and contains each such element exactly \( c_1 \) times. This "relative difference set" will be denoted by \( R(m, n, c_0, c_1) \). If \( G = \{g_1, g_2, \cdots, g_{mn}\} \) and if the elements are so ar-
ranged that for each \( i = kn + r, 0 < r \leq n, g_i + H = \{ g_j | kn < j \leq (k+1)n \} \),

define the incidence matrix \( A = (a_{ij}) \) by \( a_{ij} = 1 \) if \( g_i \in g_j + R \), \( a_{ij} = 0 \) otherwise. Then \( AA' = A'A = c_0 I_{mn} + c_1 J_{mn} - c_1 (I_m \otimes J_n) \). (Note that our ordering of the elements of \( G \) and our use of the tensor product notation \( \otimes \) differ from that of \([2]\).)

The following example generalizes a special case of the one given by Theorem 3.1 of \([2]\). Let \( A_q \) be an additive abelian group of order \( q \) for which there is a binary operation \( \circ \) satisfying

(i) \( (a+b) \circ c = (a \circ c) + (b \circ c) \),

(ii) \( a \circ (b+c) = (a \circ b) + (a \circ c) \),

(iii) For each \( 0 \neq g \in A_q \), and each \( a \in A_q \), there is a unique \( n \in A_q \) such that \( a = (n \circ g) + (g \circ n) \).

Actually this is enough to force \( g \) to be a prime power. For define a new multiplication \( * \) by: \( a * b = a \circ b + b \circ a \) for \( a, b \in A_q \). Then (i), (ii), and (iii) imply that \( (A_q, +, *) \) is a presemifield and \( A_q \) is an elementary abelian group (cf. §2 of \([4]\)).

As an example, let \( F \) be a finite field of characteristic \( p, \alpha \) an automorphism of \( F \) of odd order. Define a new multiplication \( * \) by: \( a \circ b = ab^\alpha, a, b \in F \). Then properties (i) and (ii) follow immediately since \( \alpha \) is an automorphism. To prove (iii) it suffices to show that if \( a, n_1, n_2, g \in F \) with \( g \neq 0 \) and if \( a = n_1 g^\alpha + n_2 g^\alpha + gn_2^\alpha \), then \( n_1 = n_2 \).

The assumption implies \( (n_1 - n_2)g^\alpha = (n_2^\alpha - n_1^\alpha)g \), or \( -x(x^{-1})^\alpha = g(g^{-1})^\alpha \), where \( x = n_1 - n_2 \) is assumed to be nonzero. Thus \( (gx^{-1})^\alpha = -gx^{-1} \), so \( (gx^{-1})^a = (-1)^i(gx^{-1}) \). Setting \( t \) equal to the odd order of \( \alpha \) (perhaps \( t = 1 \)), we have a contradiction for odd \( p \). This implies \( n_1 = n_2 \) and shows that \( F = A_q \) provides an example \( (A_q, +, \circ) \) satisfying (i), (ii), and (iii).

Let \( G_N \) be the direct sum of \( A_q \) taken \( N \) times, with identity \( 0 \) and whose elements are expressed as \( N \)-tuples of elements of \( A_q \). Let \( G = A_q \oplus G_N, H = A_q \oplus \{ 0 \} \). Put \( R = \{ (f(n), n) | n = (n_1, \cdots, n_N) \in G_N \} \), where \( f(n) = \sum_{i=1}^N (n_i \circ n_i) \). We claim \( R \) is an \( R(q^N, q, q^N, q^{N-1}) \) of \( G \) relative to \( H \). For let \( r(n) = (f(n), n) \) and suppose that \( (a, g) = (a, g_1, \cdots, g_N) \) is an arbitrary element of \( G \setminus H \). Then \( (a, g) = r(n + g) - r(n) \) if and only if

\[
a = \sum_{i=1}^N [(n_i + g_i) \circ (n_i + g_i) - (n_i \circ n_i)]
= \sum_{i=1}^N [(n_i \circ g_i) + (g_i \circ n_i) + (g_i \circ g_i)].
\]

By hypothesis there is some \( i \) such that \( g_i \neq 0 \). Therefore choose \( n_i, 1 \leq j \leq N, j \neq i \), arbitrarily from \( A_q \). Then for each such choice there is
a unique value of \( n_i \) in \( A_q \) satisfying

\[
a - (g_i \circ g_i) = \sum_{j=1, j \neq i}^N [(n_j \circ g_i) + (g_i \circ n_j) + (g_j \circ g_i)]
\]

\[
= (n_i \circ g_i) + (g_i \circ n_i).
\]

Hence \((a, g)\) can be expressed as a difference of two elements of \( R \) in exactly \( q^{N-1} \) ways. Clearly no element of \( H \) other than the identity can be expressed as such a difference.

We conclude with an example of an \( A \) satisfying the incidence equation \( AA' = A'A = nI + J - (I_n \otimes J_n) \). Let \( \pi \) be a projective plane of order \( n \). Then let \((x, L)\) be an incident point-line pair of \( \pi \). Let \( \pi' \) be the elliptic semiplane of type \((a)\) obtained from \( \pi \) by deleting the lines through \( x \) and the points on \( L \) (cf. [1, p. 316]).

Let \( A \) be an incidence matrix of \( \pi' \) obtained by letting points of \( \pi' \) index columns of \( A \), lines of \( \pi' \) index rows of \( A \), where the points and the lines have been grouped into parallel classes. Indeed, considering the results of Dembowski we see that the existence of a \((0, 1)\) matrix \( A \) such that \( AA' = A'A = nI + J - (I_n \otimes J_n) \) is equivalent to the existence of a projective plane of order \( n \). In this case Theorem 1.5 and Lemma 1.4 reduce to the Bruck-Ryser theorem (cf. [9, p. 115]). (We recommend [4] for a clear exposition of the rules governing the evaluation of the Hilbert symbol.)

Acknowledgment. Our thanks to the referee for several helpful comments on and corrections to the original version of this paper.

References

8. S. E. Payne and M. F. Tinsley, On \( v_1 \times v_2 \) \((n, s, t)\)-configurations, J. Combinatorial Theory 7 (1969), 1–14.

University of Miami, Coral Gables, Florida 33124

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use