On Normally Regular Digraphs

Leif K. Jørgensen
Dept. of Mathematics and Comp. Sc.
Aalborg University
Fr. Bajers Vej 7, 9220 Aalborg Ø, Denmark
e-mail: leif@iesd.auc.dk

Abstract

A normally regular digraph is a regular digraph in which the number of common out-neighbours of a pair of vertices only depends on whether the vertices are adjacent or not. In this paper we give constructions of normally regular digraphs from symmetric designs and we give some difference set constructions. For other parametersets we prove non-existence of normally regular digraphs using either combinatorial techniques or a Bruck-Ryser type theorem.

In this paper we introduce regular digraphs with the property that for every pair of distinct vertices x and y the number of vertices dominated by both x and y is λ if x and y are adjacent and it is μ otherwise, for some constants λ and μ.

The authors interest in these graphs was caused by an application (see [9]) where $\mu = 2$ and $\lambda = 0$. In the litterature they have been investigated by Ito [7] for $\mu = \lambda$ and by Fried and Sós [4] for $\mu = \lambda + 1 = 1$.

Non-symmetric association schemes with at most four classes also gives examples of normally regular digraphs; in particular a short distance regular digraph (see Damerell [2]) of girth at most five is a normally regular digraph.

The digraphs investigated in this paper do not share the property of (undirected) strongly regular graphs that the adjacency matrix has exactly three eigenvalues; for this a different restriction is needed, see Duval [3].

Although they have the property that the adjacency matrix is normal and thus diagonalizable over $\mathbb{C}$, it seems that the methods for investigating such graphs should be similar to what is used for (symmetric) designs.

1 Terminology

Let G be a finite directed graph (digraph) and let x and y be vertices of G. If there is an edge (arc) directed from x to y we say that x dominates y and write $x \to y$. By x^+ we denote the set of out-neighbours of x, i.e. the set of vertices (in G) dominated by x, or sometimes the subgraph induced by this set. By $d^+(x)$ and $d^+(x, y)$ we denote the cardinalities of x^+ and $x^+ \cap y^+$, respectively. Similarly x^-, $d^-(x)$, and $d^-(x, y)$ denotes the set of in-neighbours of x (vertices dominating x), the cardinality of x^-, and the cardinality of $x^- \cap y^-$, respectively. We say that G is regular if there is a number k so that $d^+(x) = d^-(x) = k$ for every vertex x in G.

If the vertices of G are enumerated from 1 to n, $V(G) = \{v_1, \dots, v_n\}$, then we define the adjacency matrix A of G to be the $n \times n$ matrix in which the (i, j) entry is 1 if $v_i \to v_j$ and 0 otherwise.

Let A^* denote the transpose of A. Then the (i, j) entry of AA^* is $d^+(v_i, v_j)$ and the (i, j) entry of A^*A is $d^-(v_i, v_j)$. We see that A is normal if and only if $d^+(x, y) = d^-(x, y)$ for every pair of (not necessarily distinct) vertices x and y. We say a digraph is normal if its adjacency matrix is normal, see Torgaśev [16].

A tournament is a digraph in which each pair of distinct vertices is joined by exactly one edge.

Lemma 1 ([14]) *A tournament is normal if and only if it is regular.*

Proof By the above observation a normal digraph is regular. Suppose that G is a regular tournament. Let x and y be any vertices of G. We show that $d^+(x, y) = d^-(x, y)$. This is obvious if $x = y$, so suppose that $x \neq y$. We may assume that $x \to y$.

The number of out-neighbours of y is $d^+(y)$. Of these $d^+(x, y)$ are also out-neighbours of x. The remaining $d^+(y) - d^+(x, y)$ dominate x. There are further $d^-(x) - (d^+(x) - d^+(x, y)) = d^+(x, y)$ vertices that dominate x. These are the vertices that dominate both x and y. $\diamond$

Definition *A normally regular digraph (NRD) with parameters* (v, k, λ, μ) *is a directed graph on* v *vertices without 2-cycles or multiple edges so that*

- *every vertex has out-degree* k
- *every pair of adjacent vertices has* λ *common out-neighbours*
- *every pair of non-adjacent vertices has* μ *common out-neighbours.*

Other important parameters of a normally regular digraph are $k - \mu + (\mu - \lambda)^2$ and $k + \mu - \lambda$. We denote these by η and ρ, respectively.

For a first restriction on the parameters we note that if $y \in x^+$ then as $d^+(x, y) = \lambda$, y has out-degree λ in the subgraph x^+. Since x^+ has no 2-cycles, this implies

$$k \geq 2\lambda + 1 \tag{1}$$

except in the trivial case $k = 0$.

If A is the adjacency matrix of an NRD(v, k, λ, μ) then

$$AA^* = kI + \lambda(A + A^*) + \mu(J - I - A - A^*) \tag{2}$$

where I and J are the identity and all 1 $v \times v$ matrices, respectively. It is important to note that $A+A^*$ is a $\{0, 1\}$ matrix, as the graph has no 2-cycles; otherwise the equation would not hold.

Sometimes it is convenient to to write this equation in the following form

$$(A + (\mu - \lambda)I)(A + (\mu - \lambda)I)^* = (k - \mu + (\mu - \lambda)^2)I + \mu J$$

or

$$(A + (\mu - \lambda)I)(A + (\mu - \lambda)I)^* = \eta I + \mu J \tag{3}$$

Proposition 2 *A normally regular digraph is normal.*

Proof Let $B = A + (\mu - \lambda)I$. Then $BB^* = \eta I + \mu J$. Suppose first that B is singular. Then one of the eigenvalues of $\eta I + \mu J$ is zero: $\eta = 0$ or $\eta + \mu v = 0$. Since $\mu, v \geq 0$ this is possible only when $\eta = k - \mu + (\mu - \lambda)^2$

is 0. As $k + (\mu - \lambda)^2 \geq k \geq \mu$, $\mu = k + (\mu - \lambda)^2$ implies $k = \mu = \lambda$. By equation 1 this implies $k = 0$.

Thus we may assume that B is non-singular. Since every vertex has out-degree k, we have $BJ = \rho J$, where $\rho = k + \mu - \lambda$. We get $\rho^{-1}J = B^{-1}J$ and

$$B^* = B^{-1}(BB^*) = B^{-1}(\eta I + \mu J) = \eta B^{-1} + \mu\rho^{-1}J \tag{4}$$

Using that J is symmetric, we get from this

$$\rho J = (BJ)^* = JB^* = \eta JB^{-1} + \mu\rho^{-1}J^2 = \eta JB^{-1} + \mu\rho^{-1}vJ.$$

This implies that

$$JB^{-1} = \frac{\rho - \mu\rho^{-1}v}{\eta}J,$$

and so

$$vJ = J^2 = (JB^{-1})(BJ) = \frac{\rho - \mu\rho^{-1}v}{\eta}\rho vJ.$$

Thus

$$\frac{\rho - \mu\rho^{-1}v}{\eta} = \rho^{-1}, \tag{5}$$

and $JB^{-1} = \rho^{-1}J$ or $\rho J = JB$. Now equation 4 implies

$$B^*B = \eta I + \mu\rho^{-1}JB = \eta I + \mu J = BB^*.$$

Thus we have $A^*A = AA^*$. ◇

Rewriting equation 5 we get

$$\mu v = \rho^2 - \eta. \tag{6}$$

2 NRD's with special values of μ

In this section we investigate NRD's for which μ is equal to either λ, $\lambda + 1$, 0, or k. In each of these cases we will see that there is a connection between the digraph and a symmetric design.

2.1 $\mu = \lambda$

In this case the number of common out-neighbours of a pair of vertices is constant and the graph is called doubly-regular, see Ito [7]. Ito observed that if the vertices of such a graph are $x_1, \dots, x_v$ then one can construct a symmetric $2-(v,k,\lambda)$ design with points $p_1, \dots, p_v$ and blocks $B_1, \dots, B_v$ such that $p_i \in B_i$ if and only if there is an edge from x_i to x_j.

The adjacency matrix of the graph is then an incidence matrix of the design.

Conversely, suppose that for some symmetric design there is an enumeration of points and blocks so that $p_i \notin B_i$ and if $p_i \in B_j$ then $p_j \notin B_i$. Then the incidence matrix of the design with respect to this enumeration is an adjacency matrix of an NRD with $\mu = \lambda$.

However, Ito [7] also observed that it is possible that several non-isomorphic graphs can be constructed from one design. In Table 1 there is a list of some small symmetric design. For each design (a lower bound on) the number of non-isomorphic NRD's whose adjacency matrix is an incidence matrix of the design is given. These graphs can be found be permuting the rows and columns of an incidence matrix of the design in such a way that we get a matrix with 0's on the diagonal and no pair (i,j) such that both the ij-entry and the ji-entry is 1. Since application of the same permutation to both rows and columns correspond to a permutation of the vertices of digraph, it suffices to consider all permutations of rows.

If the NRD-graph is a tournament then there are no pair of non-adjacent vertices and μ could be any number - we may take $\mu = \lambda$. Such tournaments appear in many connections and have been giving several names: Reid and Brown [13] called them doubly regular tournaments; they are called homogenous tournaments by Kotzig [11], and Ito [8] use the term Hadamard tournament, as these tournaments are equivalent to skew Hadamard matrices, see Reid and Beineke [13].

Design	v	k	λ	no. of NRD's with $\mu = \lambda$	no. of NRD's with $\mu = \lambda + 1$
PG(2,2)	7	3	1	1	1
PG(2,3)	13	4	1	4	5
PG(2,4)	21	5	1	> 1000	187
	11	5	2	1	0
PG(2,5)	31	6	1	> 1000	> 1000
B_1	16	6	2	1	2
B_2	16	6	2	2	7
B_3	16	6	2	1	7
	15	7	3	0	0
	15	7	3	1	0
	15	7	3	1	0
	15	7	3	0	0
	15	7	3	0	0

Table 1 A list of some small symmetric $2-(v,k,\lambda)$ designs with the number of non-isomorphic NRD's that can be constructed from each design using the methods of sections 2.1 and 2.2, respectively. In three cases, I havent found all the NRD's. B_i is the notation from Hall [5].

Reid and Brown also proved that doubly regular tournaments are exactly those tournaments for which there exist a constant $k > 0$ such that every edge is on exactly k directed 3-cycles. Rowlinson [14] showed doubly regular tournaments are those tournament for which there exist constants $k_4 > 0$ and $k_5 > 0$ such that every edge is on exactly k_4 4-cycles and k_5 5-cycles. Duval [3] proved that doubly regular tournaments are the only digraphs without 2-cycles which are what he called strongly regular.

2.2 $\mu = \lambda + 1$

If A is an adjacency matrix of an NRD with $\mu = \lambda + 1$ then by equation 3, $(A+I)(A+I)^* = (k+1-\mu)I + \mu J$ so that $A+I$ is the incidende matrix of a symmetric $2-(v,k+1,\mu)$ design, similar to the case $\mu = \lambda$. However, given a symmetric $2-(v,k,\lambda)$ design the inverse construction does not necessarily work (even if $v \geq 2k-1$, which is an obvious necessary condition).

In Table 1, we give the number of non-isomorphic NRD's with $\mu = \lambda + 1$ that can be constructed from small designs.

The author do not know any Hadamard-design $2-(4t-1, 2t-1, t-1)$ with $t > 2$ for which the construction works.

For projective planes the situation is quite different.

Theorem 3 (Fried and Sós [4]) *Any symmetric* $2-(k^2+k+1, k+1, 1)$ *design has an incidence matrix* A *so that* $A - I$ *is the adjacency matrix of an NRD*$(k^2+k+1, k, 0, 1)$.

In particular, there is an NRD$(k^2+k+1, k, 0, 1)$ for every prime-power k.

To prove this theorem we need P. Hall's theorem on distinct representatives of sets.

Theorem 4 ([6]) *Let $S_1, \dots, S_n$ be a family of sets. Then the following statements are equivalent*

- *There exist distinct elements $x_1, \dots, x_n$ so that for every i, $x_i \in S_i$.*
- *For any number k, $0 \le k \le n$, any subfamily of k sets have at least k elements in their union.*

If for some number r, every S_i has cardinality r and every element is in r sets then it easily shown that the second statement of Hall's theorem holds. Thus any symmetric design has an enumeration of points and blocks such that point i is in block i, and so the incidence matrix has 1's on the diagonal (similarly, it has an incidence matrix with 0's on the diagonal).

Let A be an incidence matrix of $2-(k^2+k+1, k+1, 1)$ design with 1's on the diagonal. For $A-I$ to be an adjacency matrix of an NRD we only need to prove that for $i \neq j$, A cannot have 1's on entry (i,j) and on entry (j,i). Suppose it has. Then block i and block j have two points (point i and point j) in common, a contraction. This proves Theorem 3. $\diamond$

2.3 $\mu = 0$

An NRD with $\mu = 0$ need not be connected. However, each connected component will be an NRD with the same value of k and λ. Thus we will only consider NRD's whose underlying undirected graph is connected. As each vertex has equal in- and out-degree this implies that the digraph is strongly connected. Thus there is a directed path from any vertex to any other vertex. An NRD with $\mu = 0$ may be a tournament as described in section 2.1. Another possibility is that $k = 1$ and the digraph is a directed cycle.

Suppose therefore that G is a connected NRD with $\mu = 0$, $k \ge 2$ and that G is not a tournament.

As $\mu = 0$ we get by inserting $\eta = k - \mu + (\mu - \lambda)^2 = k + \lambda^2$ and $\rho = k + \mu - \lambda = k - \lambda$ in equation 6 that $\lambda = \frac{k-1}{2}$. Let x be a vertex of G. Then every vertex in x^+ has out-degree λ in this subgraph and thus in-degree at most $k - 1 - \lambda = \lambda$. It follows that x^+ is a regular tournament. Similarly, x^- is a regular tournament.

Since G is strongly connected and it is not a tournament, there exist a vertex $y \in G$ so that x and y are non-adjacent and there is a path from x

to y in G. We may choose y so that the (directed) distance from x to y is minimal, i. e. y is dominated by a vertex in x^+ or in x^-. Since x and y are non-adjacent and $\mu = 0$, y is not dominated by any vertex in x^-, and similarly y does not dominate any vertex in x^+. Thus y is dominated by a vertex, say v, in x^+. Suppose there is a vertex w in x^+ that does not dominate y. Since x^+ is a regular tournament it is strongly connected, so there is a directed path from v to w in x^+. On this path there are vertices u and u' so that $u \to u'$, $u \to y$ but u' does not dominate y. This is a contradiction to $\mu = 0$. Thus every vertex in x^+ dominates y. If another vertex y', non-adjacent to x was dominated by a vertex in x^+, it would be dominated by every vertex in x^+ and so $d^-(y, y') = k$, a contradiction. Thus every vertex in x^+ dominates λ vertices in x^-.

Now a vertex in x^- dominated by a vertex in x^+ (which dominates y) must be adjacent to y, as $\mu = 0$. As above, y then dominates every vertex of x^-, and every vertex in x^- is dominated by λ vertices in x^+. Also every vertex in x^- dominates exactly λ vertices in x^+. Thus $V(G) = \{x, y\} \cup x^+ \cup x^-$. Furthermore there is an enumeration of vertices $x^+ = \{v_1, \dots, v_n\}$ and $x^- = \{v'_1, \dots, v'_n\}$ such that v'_i is the unique vertex non-adjacent to v_i and vice versa.

If $v_i \to v_j$ then, since no vertex dominates both v_j and v'_j, $v'_j \to v_i$. Similarly $v_j \to v'_i$ and $v'_i \to v'_j$. Thus the mapping $v_i \mapsto v'_i$ is an isomorphism.

We also see that v'_k is common out-neighbour of v_i and v_j if and only if v_k is a common in-neighbour of v_i and v_j. Thus the number of vertices in x^+ dominating v_i and v_j plus the number of vertices in x^+ dominated by v_i and v_j is $\lambda - 1$. But since x^+ is a regular tournament it is normal (by Lemma 1) and thus these two numbers are both equal to $\frac{\lambda-1}{2}$ and so λ is odd, and x^+ is a doubly regular tournament, $\mathrm{NRD}(k, \lambda, \frac{\lambda-1}{2}, \cdot)$.

If on the other hand G is a doubly regular tournament with degree $k = 2\lambda + 1$ and with vertex-set $\{x_1, \dots, x_n\}$, $n = 2k + 1$, then we may construct a graph with vertex-set $\{v_0, \dots, v_n, v'_0, \dots, v'_n\}$ and edges

$$v_0 \to v_i \to v'_0 \to v'_i \to v_0, \text{ for } 1 \le i \le n$$

and

$$v_i \to v_j \to v'_i \to v'_j \to v_i \text{ if } x_i \to x_j \text{ in } G, \text{ for } 1 \le i, j \le n.$$

It is easy to check that this new graph is an $\mathrm{NRD}(2n + 2, n, k, 0)$.

This characterization can be formulated in terms of matrices:

Theorem 5 *A connected digraph is an NRD with $\mu = 0$ if and only if either*

1. *it is a directed cycle ($k = 1$)*
2. *it is a doubly regular tournament or*
3. *it has an adjacency matrix of the following form*

$$\begin{pmatrix} 0 & 1 \ldots 1 & 0 & 0 \ldots 0 \\ 0 & & 1 & \\ \vdots & A & \vdots & A^* \\ 0 & & 1 & \\ 0 & 0 \ldots 0 & 0 & 1 \ldots 1 \\ 1 & & 0 & \\ \vdots & A^* & \vdots & A \\ 1 & & 0 & \end{pmatrix}$$

where A is an adjacency matrix of a doubly regular tournament.

The graph in Figure 1 is the smallest example of the type of NRD mentioned as possibility 3. This graph is a Cayley graph of the quarternion group.

In [10], it is investigated when NRD's of this type are vertex transitive.

Figure 1 An NRD$(8, 3, 1, 0)$.

The connection between skew Hadamard matrices and the digraphs of type 3 in the above theorem is as follows: Let H be an $n \times n$ skew Hadamard matrix, i. e., a ± 1 matrix such that that $HH^* = nI$ and $H + H^* = 2I$. Then we may assume that the entries of the first row of H are 1. Let M be the matrix obtained from H by replacing each -1 and each diagonal entry by 0. Then

$$\begin{pmatrix} M & M^* \\ M^* & M \end{pmatrix}$$

is the adjacency matrix of a digraph of type 3 in the theorem.

Conversely, from the submatrix

$$\begin{pmatrix} 0 & 1 \dots 1 \\ 0 & \\ \vdots & A \\ 0 & \end{pmatrix}$$

of the matrix in the theorem, we obtain a skew Hadamard matrix by setting the diagonal enties to 1 and replacing every other 0 entry by -1.

2.4 $\mu = k$

Theorem 6 *A graph G is an NRD with $\mu = k$ if and only if there is a number s so that G is obtained from a doubly-regular tournament by replacing each vertex x by a set V_x of s new vertices such that if $x \to y$ in the tournament then $u \to w$ for every $u \in V_x$ and $w \in V_y$. Then $s = k - 2\lambda = v - 2k$.*

In other words a graph is an NRD with $\mu = k$ if and only if it has an adjacency matrix which is the Kronecker produkt (see Hall [5]) of an adjacency matrix of a doubly regular tournament and the all one $(s \times s)$ matrix.

Proof It is easy to check that every graph obtained from an NRD$(v, k, \lambda, \cdot)$-tournament as described is an NRD$(sv, sk, s\lambda, sk)$.

Suppose now that G is an NRD with $k = \mu$. Suppose that x and y are non-adjacent vertices. Then, as $\mu = k$, every vertex dominating x also dominates y. If z is another vertex non-adjacent to x, then every vertex dominating x also dominates z, so that $d^-(y, z) = k$. Since $\lambda \leq \frac{k-1}{2}$, y and z are non-adjacent. Non-adjacency is thus a transitive relation on the vertex-set, which is therefore partitioned into classes, say $V_1, \dots, V_r$, such that any two vertices are adjacent if and only if they belong to distinct classes.

Suppose that $x \in V_i$ dominates $y \in V_j$, for some $1 \leq i, j \leq r$. Then every vertex in V_i dominates every vertex in V_j. For let $x' \in V_i$ and $y' \in V_j$ be any vertices, then if $x \neq x'$, x and x' are non-adjacent and have the same out-neighbours, so that $x' \to y$ and similarly $x' \to y'$. We also have

$$2k = d^-(x) + d^-(y) = v - |V_j|$$

since every vertex of G dominates either x or y, except for the vertices in V_j and the λ vertices that are dominated by both x and y, and since λ vertices dominates both x and y. Similarly:

$$2k = d^+(x) + d^+(y) = v - |V_i|.$$

It follows that $|V_i| = |V_j| = v - 2k$. Denote this number by s. Then s divides k and λ. The digraph with vertex-set $\{V_1, \dots, V_r\}$ and edges $V_i \to V_j$ if the vertices of V_i dominates the vertices of V_j in G, is obviously a doubly-regular tournament with degree $\frac{k}{s}$ and double-degree $\frac{\lambda}{s}$, so that $\frac{k}{s} = 2\frac{\lambda}{s} + 1$ and $k = 2\lambda + s$. $\diamond$

3 Non-existence results

In this section we prove non-existence of NRD's with certain parametersets. First we give a Bruck-Ryser type restriction on the parameters and then after considering the eigenvalues of an NRD we give a combinatorial proof to exclude some other parametersets.

3.1 A Bruck-Ryser type theorem

Theorem 7 *Suppose that there exist an NRD(v, k, λ, μ).*

- *If v is even then $\eta = k - \mu + (\mu - \lambda)^2$ is a square.*
- *If $v \equiv 1 \pmod 4$ then the Diophantine equation $x^2 - \mu y^2 = \eta z^2$ has an integer solution such that x, y, and z are not all zero.*
- *If $v \equiv 3 \pmod 4$ then the Diophantine equation $x^2 + \mu y^2 = \eta z^2$ has an integer solution such that x, y, and z are not all zero.*

Proof It follows from equation 3 that the determinant of $\eta I + \mu J$ is a square. The eigenvalues of this matrix are $\eta + \mu v = \rho^2$ with multiplicity 1 and η with multiplicity $v - 1$. For the equality we used equation 6. Thus the result follows when v is even.

For v odd, the theorem follows from equation 3 and the following lemma.

Lemma 8 ([1]) *Suppose that N is a rational $v \times v$ matrix satisfying the equation*

$$NN^* = (a-b)I + bJ$$

for some integers $a > b$ and v odd. Then the equation

$$x^2 = (a-b)y^2 + (-1)^{(v-1)/2}bz^2$$

has a solution $(x, y, z) \in \mathbb{Z}^{\not\models} \setminus \{(\not\vdash, \not\vdash, \not\vdash)\}$.

3.2 Eigenvalues of NRD's

From the observation in the above proof about the spectrum of the right hand side of equation 3 we can prove a restriction on the spectrum of the adjacency matrix A of an NRD(v, k, λ, μ).

Let x be an eigenvector for A with eigenvalue θ. Then it is well-known from linear algebra that x is an eigenvector for A^* with eigenvalue $\overline{\theta}$, as A is normal.

Thus $(\theta+\mu-\lambda)(\overline{\theta}+\mu-\lambda)$ is an eigenvalue of $(A+(\mu-\lambda)I)(A+(\mu-\lambda)I)^*$.

If $\theta = k$ the all entries of x are equal and

$$(k + \mu - \lambda)^2 = \eta + \mu v$$

(this is in fact equation 6).

If $\theta \neq k$ then

$$(\theta + \mu - \lambda)(\overline{\theta} + \mu - \lambda) = \eta$$

or

$$|\theta - (\lambda - \mu)| = \sqrt{\eta} \tag{7}$$

so that the eigenvalues lie on a circle in the complex plane with centre $\lambda - \mu$ and radius $\sqrt{\eta}$.

This seems to be all that we can say in general about the the spectrum of an NRD. Examples show that the parameters do not determine the spectrum.

However, in the cases $\mu = k$ and $\mu = 0$ we may use the characterization in the previous section to calculate the spectrum.

Let A be the adjacency matrix of an NRD with $\mu = k$ obtained from a doubly regular tournament with degree $k' = 2\lambda' + 1$ by replacing each vertex by s vertices. For vertices x and y we need to find the number of paths from x to y of length 2. If x and y are non-adjacent then there are none; otherwise the number is s times the number of paths of length 2 in the tournament from the vertex corresponding to x to the vertex corresponding to y, i. e. it is $s\lambda'$ if $x \to y$ and it is $s(\lambda'+1)$ if $y \to x$. It follows that

$$A^2 = s\lambda' A + s(\lambda'+1)A^*$$

and that an eigenvalue θ of A satisfies

$$\theta^2 = s\lambda'\theta + s(\lambda'+1)\overline{\theta}.$$

By solving this equation, we find that the eigenvalues of A are:

$$k,\ 0,\ -\frac{1}{2}s(1+i\sqrt{4\lambda'+3}),\ -\frac{1}{2}s(1-i\sqrt{4\lambda'+3})$$

As the sum of the eigenvalues is zero, the multiplicities are 1, $(s-1)(2k'+1)$, k', and k', respectively, i. e. 0 is not an eigenvalue for $s=1$.

Now let A be the adjacency matrix of an NRD with $\mu = 0$ that is not a tournament (which is the above case with $s=1$).

Then we get

$$A^2 = \lambda(A+A^*) + k(J - A - A^* - I)$$

and for an eigenvalue $\theta \neq k$:

$$\theta^2 = \lambda(\theta+\overline{\theta}) - k(\theta+\overline{\theta}+1) = -(\lambda+1)(\theta+\overline{\theta}) - k$$

When $\mu = 0$ we get from equation 6 (or from section 2.1) that $k = 2\lambda+1$. Inserting in equation 7 gives:

$$|\theta - \lambda| = \sqrt{k+\lambda^2} = \sqrt{\lambda^2+2\lambda+1} = \lambda+1.$$

Solving these equations equations we find that the eigenvalues of A are :

$$k,\ -1,\ i\sqrt{k},\ -i\sqrt{k}$$

As the sum of the eigenvalues is 0, the multiplicities are:

$$1,\ k,\ \lambda+1,\ \lambda+1.$$

3.3 Combinatorial investigation

The Bruck Ryser type theorem in the previous section leaves open the existence of NRD's for many parametersets, where no NRD has been constructed. Here we use combinatorial methods to investigate some such parametersets with $\lambda = 0$.

Theorem 9 *If an NRD with $\lambda = 0$, $\mu \neq k$ and $\mu \geq 2$ exists then $k > 2\mu + \frac{1}{2} + \sqrt{2\mu + \frac{1}{4}}$.*

From Theorem 6 we know that an NRD$(v, k, 0, k)$ is obtained from a directed triangel by replacing each vertex by k vertices.

Proof Suppose that G is an NRD$(v, k, 0, \mu)$ with $\mu \neq k$. In this proof we use notation $U_x = V(G) - \{x\} - x^+ - x^-$ for a vertex x in G. By equation 6 we have

$$|U_x| = \frac{k(k-1)}{\mu} \tag{8}$$

It is obvious that $k > \mu$.

Claim 1: $k \geq 2\mu$.

Proof Suppose that $\mu < k < 2\mu$, and let $x \in V(G)$. If $y \in U_x$ then as x and y have μ common out-neighbours, y dominates μ vertices in x^+. As $2\mu > k$ any two vertices in U_x have a common out-neighbour in x^+. As $\lambda = 0$, this implies that U_x is an independent set.

Let $z \in x^+$. Every vertex other than x dominating z belong to U_x. As U_x is independent, no vertex dominates both z and $y \in U_x$ and so z is adjacent to every vertex in U_x (but to no other vertex in x^+). Thus z is adjacent to $2k - 1 - |U_x|$ vertices in x^-. By equation 8 and $\mu < k < 2\mu$, we have $k > 2k - 1 - |U_x| > 1$, and so there is a vertex $w \in x^-$ adjacent to z and a vertex $u \in x^-$ not adjacent to z. Then w and z are adjacent vertices in U_u, a contradcition.

Claim 2: $k > 2\mu$.

Proof Suppose that $k = 2\mu$ and $k > 2$. Let x be any vertex in G. By equation 8, $|U_x| = 2k - 2$. Suppose that $y, z \in U_x$ and y dominates z. $x^+ \cap y^+$ and $x^+ \cap z^+$ are disjoint sets (as $\lambda = 0$) of cardinality μ. Thus their union is x^+. z has μ in-neighbours in x^-, no in-neighbours in x^+ and thus μ in-neighbours in U_x. Let $y' \in U_x$ be another vertex dominating z. Then

y' and z have no common out-neighbours in x^+, i.e. $x^+ \cap (y')^+ = x^+ \cap y^+$. Thus y and y' have at least $\mu + 1$ common out-neighbours, a contradiction.

Thus U_x is an independent set. As in the previous case, every vertex in x^+ is adjacent to every vertex in U_x and thus it dominates exactly one vertex in x^-. By symmetry, every vertex in x^- is dominated by exactly one vertex in x^+, and so the edges between x^+ and x^- form a matching. A vertex in U_x dominates μ vertices in x^+ and those μ vertices in x^- that are not matched to the out-neighbours in x^+, as $\lambda = 0$. It follows that any two vertices in U_x have exactly $\frac{\mu}{2}$ common out-neighbours in x^+ and $\frac{\mu}{2}$ common out-neighbours in x^-. Thus we consider U_x and x^+ to be points and blocks of a 2-design in which a block is incident to the points by which it is dominated in G. By Fisher's inequality (see Hall [5]) we have $k \geq 2k - 2$ and thus $k \leq 2$, a contradiction.

Claim 3: $k > 2\mu + 1$.

Proof Suppose that $k = 2\mu+1$ and let x be a vertex in G. By equation 8, $|U_x| = 2k$. Since G is regular and $|U_x \cup \{x\}| > |x^+ \cup x^-|$, U_x cannot be an independent set. Let $y, z \in U_x$ so that $y \to z$. y and z have no common out-neighbours in x^+ so there a unique vertex $w \in x^+$ which is not dominated by y or z. The in-neighbours of z are μ vertices in x^-, possibly w, and at least μ vertices in U_x. Let $y' \neq y$ be a vertex in U_x dominating z. Since y' and z have no common out-neighbours in x^+ and y and y' have only μ common out-neighbours, y' dominates w. Since $\lambda = 0$, w does not dominate z, and so z has $\mu + 1$ in-neighbours in U_x. We have now shown that in the graph spanned by U_x any vertex has in-degree either 0 or $\mu + 1$ and, by symmetry, it has out-degree either 0 or $\mu+1$. Thus the in-neighbours of z in U_x has out-degree $\mu+1$. Any two in-neighbours of z in U_x have at least $\mu-1$ commmon out-neighbours $(x^+ \cap y^+) \cup \{w\}$. Thus z is their only common out-neighbour in U_x. Counting the vertices in U_x we have

$$4\mu + 2 = |U_x| \geq 1 + (\mu + 1) + (\mu + 1)\mu,$$

and so $\mu = 2$.

Now $|U_x| = 10$ and we have at least 7 vertices of in-degree 3 in U_x and, by symmetry, at least 7 vertices of out-degree 3. So there is a vertex with out-degree and in-degree 3. We may assume that z is such a vertex. Then z dominates a vertex which is also dominated by an in-neighbour of z. This is a contradiction to $\lambda = 0$. This proves claim 3.

Let $r = k - 2\mu$. Then $r \geq 2$, by Claim 3. By equation 8, μ divides $k(k-1) = (2\mu + r)(2\mu + r - 1) = \mu(4\mu + 4r - 2) + r(r-1)$. Thus μ divides $r(r-1)$ and so $r^2 - r = s\mu$, for some positive integer s. Then $r = \frac{1}{2} + \sqrt{s\mu + \frac{1}{4}}$.

If $s = 1$ then $\mu = r(r-1)$ and $k = 2\mu + r = r(2r-1)$. From equation 8, we see that $v = 1 + 2k + \frac{k(k-1)}{\mu} = 2k + 4r^2$ is even and so η is a square, by Theorem 7. But $\eta = k - \mu + \mu^2 = r^2((r-1)^2 + 1)$ cannot be a square. Thus $s \geq 2$. This proves the theorem. $\diamond$

v	k	λ	μ	NRD exists ?	Comment
10	3	0	2	no	Theorems 7 and 9
15	4	0	2	no	Theorem 9
13	4	0	3	no	Theorem 7 and 9
21	5	0	2	no	Theorem 9
16	5	0	4	no	Theorem 7 and 9
28	6	0	2	no	Theorem 7 and 9
23	6	0	3	no	Theorem 9
19	6	0	5	no	Theorems 7 and 9
19	6	1	3	yes	Theorem 13
19	6	2	1	no	Theorem 7
36	7	0	2	yes	Constructed by P. Cameron
29	7	0	3	no	Theorem 9
22	7	0	6	no	Theorems 7 and 9
22	7	1	4	no	Theorem 7
29	7	2	1	yes	Theorem 12

Table 2 A list of all parametersets (v, k, λ, μ) with $\mu \notin \{\lambda, \lambda+1, 0, k\}$ and $k \leq 7$ for which equation 6 holds. The graph with $(v, k, \lambda, \mu) = (19, 6, 1, 3)$ is unique with these parameters. The proof of this combinatorial - similar the proof of Theorem 9. For $k = 8$, there are 10 possible parametersets. Very little is known about these cases.

4 Normally regular Cayley digraphs

Let G be a group and let S be a subset of G. Then the Cayley graph $\mathrm{Cay}(G, S)$ is the graph whose vertices are the elements of G and so that

x dominates y if $x^{-1}y \in S$. In this section we investigate when a Cayley graph is an NRD. As we want to look at digraphs with no directed 2-cycle, S and S^{-1} should be disjoint, where $S^{-1} = \{s^{-1} \mid s \in S\}$. It is easy to see that $\mathrm{Cay}(G, S)$ is an $\mathrm{NRD}(|G|, |S|, \lambda, \mu)$ if and only if in the *multiset* $\{xy^{-1} \mid x, y \in S\}$ the identity of the group occurs $|S|$ times, an element in $S \cup S^{-1}$ occurs λ times, and other elements occurs μ times. If $\mu = \lambda$ then S is just an ordinary difference set (see [1]). If $\mu = \lambda + 1$ then if we add the identity to S we get again a difference set.

For some other values of μ we have the following variant of a multiplier theorem for difference sets (see [1]).

Theorem 10 *Suppose that G is an abelian group and that $Cay(G, S)$ is an $NRD(v, k, \lambda, \mu)$. Let w be the smallest positive number so that g^w is the group identity for every $g \in G$. Let m be a natural number relatively prime to v, so that m divides η and let t be relatively prime to v.*

Suppose that for every prime p dividing m there exist an integer f so that $t \equiv p^f \mod w$. If either $m > \mu \geq \lambda + 2$ or $m > 2\lambda - \mu$, $\lambda > \mu$ then $tS = S$.

Proof In the proof we use multiplicative notation for the group G. As in the case of ordinary difference sets, we consider the group ring $\mathbb{ZG}$ whose elements are formal sums
$$\varepsilon = \sum_{g \in G} c_g g,$$
where $c_g \in \mathbb{Z}$. For an integer s we use the notation
$$\varepsilon^{[s]} = \sum_{g \in G} c_g g^s$$

Then as G is abelian the mapping $\varepsilon \mapsto \varepsilon^{[s]}$ is an automorphism of G thus of $\mathbb{ZG}$, for s relatively prime to v. We define γ and σ as follows
$$\gamma = \sum_{g \in G} g, \quad \sigma = \sum_{g \in S} g.$$

The fact that $\mathrm{Cay}(G, S)$ is an $\mathrm{NRD}(v, k, \lambda, \mu)$ is equivalent to the following
$$\sigma\sigma^{[-1]} = k + \lambda(\sigma + \sigma^{[-1]}) + \mu(\gamma - \sigma - \sigma^{[-1]} - 1)$$

where the group identity is denoted by 1 and $a1$ is denoted by a for $a \in \mathbb{Z}$. If we introduce $\pi = \sigma + \mu - \lambda$ this is equivalent to

$$\pi\pi^{[-1]} = \mu\gamma + \eta \tag{9}$$

Consider the automorphism $g \mapsto g^t$ of G and let n denote its order. If α denotes $\pi^{[t]}\pi^{[-1]} - \mu\gamma$ then

$$\alpha \equiv \pi^{[t]}\pi^{[-1]} \mod \gamma$$

(to say that two elements of $\mathbb{ZG}$ are equivalent modulo some $\phi \in \mathbb{ZG}$ means that their difference has the form $\psi\phi$ for some $\psi \in \mathbb{ZG}$) and so we get the following equivalence modulo γ using that $\mathbb{ZG}$ is commutative

$$\begin{aligned} \alpha\alpha^{[t]} \ldots \alpha^{[t^{n-1}]} &\equiv \pi^{[t]}\pi^{[-1]}\pi^{[t^2]}\pi^{[-t]} \ldots \pi^{[t^n]}\pi^{[-t^{n-1}]} \\ &\equiv (\pi\pi^{[-1]})(\pi\pi^{[-1]})^{[t]} \ldots (\pi\pi^{[-1]})^{[t^{n-1}]} \\ &\equiv (\mu\gamma + \eta) \ldots (\mu\gamma + \eta)^{[t^{n-1}]} \end{aligned}$$

by equation 9. Using that $g \mapsto g^t$ is an automorphism we see that this is equivalent modulo γ to

$$(\mu\gamma + \eta)^n \equiv \eta^n$$

Thus $\alpha\alpha^{[t]} \ldots \alpha^{[t^{n-1}]} = \eta^n + \xi\gamma$ for some $\xi \in \mathbb{ZG}$. We want to show that $\xi\gamma = 0$.

Let $P : \mathbb{ZG} \mapsto \mathbb{Z}$ be the homomorphism defined by $P(\sum c_g g) = \sum c_g$. Then

$$P(\alpha) = P(\pi^{[t]}\pi^{[-1]} - \mu\gamma) = (k + \mu - \lambda)^2 - \mu v = \eta$$

by equation 6. And

$$\begin{aligned} \eta^n = P(\alpha)^n = P(\alpha)P(\alpha^{[t]}) \ldots P(\alpha^{[t^{n-1}]}) = \\ P(\alpha\alpha^{[t]} \ldots \alpha^{[t^{n-1}]}) = P(\eta^n + \xi\gamma) = \eta^n + P(\xi)v \end{aligned}$$

Thus $P(\xi) = 0$ and so $\xi\gamma = 0$ and we get

$$\alpha\alpha^{[t]} \ldots \alpha^{[t^{n-1}]} = \eta^n \tag{10}$$

We next need two properties of $\mathbb{ZG}$ (see [1, Lemmas VI.3.6 and VI.3.7]). The first is an easy application of Fermats Little Theorem and the second follows from the first. For any $\varepsilon \in \mathbb{ZG}$, a prime p not dividing v and a natural number s

$$\varepsilon^{[p^s]} \equiv \varepsilon^{p^s} \mod p \tag{11}$$

$$\varepsilon^s \equiv 0 \mod p \implies \varepsilon \equiv 0 \mod p \tag{12}$$

Let p^s be the highest power of the prime p dividing m and let p^r be the highest power of p dividing α, i. e. $\alpha = p^r\beta$ for some $\beta \in \mathbb{ZG}$. As $t \equiv p^f \mod w$, we see that $\beta^{[t]} = \beta^{[p^f]}$. Using this and equation 10 we see that p^{sn} divides

$$\eta^n = \alpha \dots \alpha^{[t^{n-1}]} = p^{rn}\beta \dots \beta^{[t^{n-1}]} = p^{rn}\beta\beta^{[p^f]} \dots \beta^{[p^{f(n-1)}]} \tag{13}$$

As p does not divide β, it follows from equation 12 that it does not divide

$$\beta^{1+p^f+\dots+p^{f(n-1)}} = \beta\beta^{p^f} \dots \beta^{f(n-1)}$$

which by equation 11 is equivalent modulo p to

$$\beta\beta^{[p^f]} \dots \beta^{[p^{f(n-1)}]}$$

Thus, by equation 13, $r \geq s$ and so $\alpha \equiv 0 \mod p^s$. As this holds for every prime dividing m, we have $\alpha \equiv 0 \mod m$. From the definition of α we get

$$\pi^{[t]}\pi^{[-1]} = \mu\gamma + m\omega \tag{14}$$

for some $\omega \in \mathbb{ZG}$. If $\mu > \lambda$, the coefficients of π are non-negative, and so are the coeffients of $\pi^{[t]}\pi^{[-1]}$. As $m > \mu$, this implies that the coefficients of ω are non-negative. If $\mu < \lambda$ then the coefficients of $\pi^{[t]}\pi^{[-1]}$ are greater than or equal to $2(\mu - \lambda)$. As $m > \mu - 2(\mu - \lambda)$ the coefficients of ω are again non-negative.

Applying P to equation 14 we get

$$\rho^2 = (k + \mu - \lambda)^2 = P(\pi^{[t]}\pi^{[-1]}) = \mu v + mP(\omega)$$

Now we get from equation 6 that

$$mP(\omega) = \eta$$

which implies that

$$m\omega\gamma = \eta\gamma \tag{15}$$

Applying the automorphism $g \mapsto g^{-1}$ to this gives

$$m\omega^{[-1]}\gamma = \eta\gamma \tag{16}$$

Applying the automorphisms $g \mapsto g^{-1}$ and $g \mapsto g^t$ to equations 14 and 9, respectively we get

$$\pi^{[-t]}\pi = \mu\gamma + m\omega^{[-1]} \tag{17}$$

and

$$\pi^{[t]}\pi^{[-t]} = \mu\gamma + \eta \tag{18}$$

Multiplying equation 9 and 18 and multiplying 14 and 17 and using commutativity of $\mathbb{ZG}$ we get

$$(\mu\gamma + \eta)^2 = (\pi\pi^{[-1]})(\pi^{[t]}\pi^{[-t]}) = (\pi^{[t]}\pi^{[-1]})(\pi^{[-t]}\pi) = (\mu\gamma + m\omega)(\mu\gamma + m\omega^{[-1]})$$

Applying 15 and 16 to this we get

$$\eta^2 = m^2\omega\omega^{[-1]} \tag{19}$$

As the coefficients of ω and $\omega^{[-1]}$ are non-negative and $\omega\omega^{[-1]}$ is a constant only one coefficient of ω can be non-zero. Thus there exist $g \in G$ and $c \in \mathbb{Z}$ so that $\omega = cg$. From equation 19 we see that $\eta^2 = m^2c^2gg^{-1} = m^2c^2$ so that $\eta = mc$. We can now rewrite equation 14

$$\pi^{[t]}\pi^{[-1]} = \mu\gamma + m\omega = \mu\gamma + \eta g$$

Multiplying this by π we get

$$(\mu\gamma + \eta g)\pi = \pi^{[t]}\pi^{[-1]}\pi = \pi^{[t]}(\mu\gamma + \eta)$$

by 9. This reduces to

$$\pi^{[t]} = g\pi$$

As the group identity is the unique element that has coefficient different from 0 and 1 in π and also in $\pi^{[t]}$ we must have $g = 1$. This proves the theorem. $\diamond$

Theorem 11 *Suppose that an NRD(v, k, λ, μ) is a Cayley graph of some abelian group G and suppose that p is a prime that divides both η and ρ but not $v = |G|$. Then p^2 divides $\mu\eta$.*

Proof With the notation of the previous proof we still have

$$\pi\pi^{[-1]} = \mu\gamma + \eta \quad \text{and} \quad \pi^{[p]}\pi^{[-p]} = \mu\gamma + \eta$$

From equation 11 we get $\pi^p \equiv \pi^{[p]} \mod p$. We have the following equivalence modulo p

$$\pi^{[p]}\pi^{[-1]} \equiv \pi^p\pi^{[-1]} = \pi^{p-1}(\pi\pi^{[-1]}) =$$
$$\pi^{p-1}(\mu\gamma + \eta) \equiv \mu\pi^{p-1}\gamma = \mu\rho^{p-1}\gamma \equiv 0$$

as p divides η and ρ. Thus there exist $\theta \in \mathbb{ZG}$ such that $\pi^{[p]}\pi^{[-1]} = p\theta$ and then $\pi^{[-p]}\pi = p\theta^{[-1]}$. Multiplying these two equations we get

$$p^2\theta\theta^{[-1]} = \pi^{[p]}\pi^{[-1]}\pi^{[-p]}\pi = (\mu\gamma + \eta)^2 = (\mu^2 v + 2\eta\mu)\gamma + \eta^2$$

Thus p^2 divides

$$\mu^2 v + 2\eta\mu + \eta^2 = \mu\rho^2 + \mu\eta + \eta^2$$

by equation 6. As p divides η and ρ, p^2 divides $\mu\eta$. $\diamond$

Example For $(k, \lambda, \mu) = (16, 3, 8)$, $\eta = 33$ and $\rho = 21$ are divisible by 3, but $\mu\eta = 264$ is not divisible by 9. However the Diophantine equation $x^2 + 8y^2 = 33z^2$ from Theorem 7 has a solution $(x, y, z) = (5, 1, 1)$. Thus an NRD with these parameters may exist but it is not a Cayley graph of an abelian group. $\diamond$

Theorem 12 *Suppose that v is a prime power, $v \equiv 5 \mod 8$. Let D denote the following subset of GF[v]:*

$$D = \{x^4 \mid x \neq 0\}$$

Then the Cayley graph of the additive group of GF[v] generated by D is an NRD with $v = 4k + 1 = 8(\mu + \lambda) + 5$.

Proof As $v \equiv 5 \mod 8$, the set D has cardinality $k = \frac{v-1}{4}$ and $-1 \notin D$. Thus $D \cup -D$ is the set of squares in $GF[v]$. This means that the cosets of the subgroup (of the multiplicative group) D are D, $-D$, R, and $-R$ for some set R. Let $D = \{1, q_2, \ldots, q_k\}$. Then $qq_i - q$, $2 \leq i \leq k$, $q \in D$ is the set of differences, we want to consider. For a fixed i, every element in the coset to which $q_i - 1$ belongs appears exactly once as a difference $qq_i - q$, $q \in D$. This means that if among the differences $q_2 - 1, \ldots, q_k - 1$, the number of elements in $D, -D, R$ and $-R$, are $\lambda_1, \lambda_2, \mu_1$ and μ_2, respectively, then among all differences of distinct element of D an element appears $\lambda_1, \lambda_2, \mu_1$, or μ_2 according to whether it belongs to $D, -D, R$, or $-R$. Since for every x, x and $-x$ appears as a difference the same number of times, $\lambda_1 = \lambda_2$ and $\mu_1 = \mu_2$. $\diamond$

The digraph constructed in Theorem 12 can be shown to be one of the classes of an association scheme.

4.1 Cayley digraphs of cyclic groups

In the construction in previous theorem the group was an elementary abelian group. When v is a prime it is a cyclic group. We shall now look at some other cyclic NRD's, i. e. NRD's that are Cayley digraphs of cyclic groups.

Theorem 13 *Let k be a multiple of 3 such that $k+1$ is a prime power. Then there exist a cyclic NRD$(\frac{k^2+3k+3}{3}, k, 1, 3)$.*

Proof When $\lambda = 1$ and $\mu = 3$, $\eta = k+1$, which is assumed to be a prime power. By equation 6, $v = \frac{\eta^2+\eta+1}{3}$.

By Singer's theorem [15] there exist a cyclic planar difference set of order η, i. e. a subset D of $\mathbb{Z}_{\nvDash\succapprox}$ with $|D| = \eta + 1$ such that each non-zero element of $\mathbb{Z}_{\nvDash\succapprox}$ is a difference of exactly one pair of elements in D. In particular there is a unique pair of difference v. By adding a constant to D if necessary, we may assume that $v, 2v \in D$. Let $D' = D \setminus \{v, 2v\}$, and let $S \subseteq \mathbb{Z}_{\succapprox}$ be the numbers congruent to numbers in D' modulo v.

As v is not a difference in D', $|S| = \eta - 1 = k$.

Suppose that x and $-x$ are both in S. Then for some $a, b \in \{0, 1, 2\}$, $x + av, -x + bv \in D'$. Choose $i, j \in \{1, 2\}$ so that $a + b \equiv i + j \pmod 3$. Then we have two equal differences in D

$$(x + av) - iv = jv - (-x + bv)$$

a contradiction. Thus $S \cap -S = \emptyset$.

If $x \in \mathbb{Z}_{\succsim}$ is congruent (mod v) to a difference of elements in D, one of which is v or $2v$, then either $x \equiv a - iv$ or $x \equiv iv - a$ for $a \in D$ and $i \in \{1, 2\}$, i. e. x or $-x \in S$. Conversely if $x \in S$ or $-x \in S$ then x is in exacty to ways congruent (mod v) to a difference of two elements in D one of which is v or $2v$.

Let $x \in \mathbb{Z}_{\succsim} \setminus (\mathbb{S} \cup -\mathbb{S} \cup \{\nvdash\})$. Then each of x, $x+v$ and $x+2v$ can be written in exacty one way as a difference of elements in D, in fact in D'. Thus x can be written in exacty three ways as a difference of elements in S.

If $x \in S \cup -S$ then only one of the three pairs of elements in D whose difference is congruent to x (mod v) is in D'. Thus x can be written in exactly one way as a difference of elements in S.

Hence $\mathrm{Cay}(\mathbb{Z}_{\succsim}, \mathbb{S})$ is an NRD$(v, k, 1, 3)$. $\diamond$

v	k	λ	μ	η	Reference
19	6	1	3	7	Theorem 13
29	7	2	1	7	Theorem 12
61	12	1	3	13	Theorem 13
31	12	4	6	10	Example 1
53	13	2	4	13	Theorem 12
91	15	1	3	16	Theorem 13
61	15	4	3	13	Theorem 12
127	18	1	3	19	Theorem 13
217	24	1	3	25	Theorem 13
151	30	4	7	32	Example 2

Table 3 A list of cyclic NRD's with $\mu \notin \{\lambda, \lambda+1, 0, k\}$. It contains all examples with $k \leq 30$ known to the author. It can be shown that the list is complete for $k \leq 15$.

In addition to these two infinite families of cyclic NRD's, I know of two more examples.

Example 1 The graph $\mathrm{Cay}(\mathbb{Z}_{\nVdash\nVdash}, \mathbb{S})$ is an NRD(31,12,4,6), where

$$S = \{1, 3, 5, 8, 9, 11, 13, 14, 15, 24, 25, 27\}$$

In this case $\eta = 10$. By Theorem 10 any prime divisor of η greater than μ is a multiplier of S. No such prime exists, however 5 is multiplier ($5S = S$) but 2 is not ($2S \neq S$).

Example 2 The graph $\mathrm{Cay}(\mathbb{Z}_{151}, \mathbb{S})$ is an NRD$(151, 30, 4, 7)$, where

$$S = \{1, 2, 4, 8, 16, 32, 64, 128, 105, 59, 118, 85, 19, 38, 76,$$
$$148, 145, 139, 127, 13, 55, 110, 69, 138, 125, 99, 47, 94, 37, 74\}).$$

4.2 Nonexistence of certain cyclic NRD's

As mentioned above it can be shown that the list of cyclic NRD's in Table 3 is complete for $k \leq 15$. In the table below it is indicated how this is done. For each value of k (column 1) the number of parametersets (v, k, λ, μ) with $\mu \notin \{\lambda, \lambda + 1, 0, k\}$ that satisfies equation 6 is found (column 2). In column 3 we see the number of parametersets for which there exist an NRD that is a Cayley digraph of a cyclic group. The number of parametersets that can be excluded by Theorems 7 and 9 is in column 4. From Theorem 10 we get a (possibly empty) set of numbers t so that $S = tS$. If -1 is among those number we have a contradiction to $S \cap -S = \emptyset$. Column 5 shows the number of parametersets that can be excluded in this way and that was not excluded in column 4.

Suppose that the parameterset has not yet been excluded and there is a number t so that $S = tS$ and $t \neq \pm 1$. Then multiplication by t is a permutation that partitions $\mathbb{Z}_v$ into disjoint cycles. Each cycle is either a subset of S or disjoint from S. The number of cycles is so small that each possible combination can be checked (on a computer). Column 6 shows the number of parametersets that can be excluded this way. Among the remaining cases, three can be excluded by Corollary 15 below. There are now nine parametersets left:

$$(36, 7, 0, 2), (21, 8, 3, 2), (55, 9, 0, 2),$$

$$(36, 10, 3, 2), (27, 10, 3, 5), (40, 13, 3, 6)$$

and

$$(55, 12, 3, 2), (120, 14, 0, 2), 64, 14, 4, 2).$$

In the first six cases v and k are so small that it is possible check each k-subset, S of $\mathbb{Z}_{\underset{\approx}{\succsim}}$ with the property that $S \cap -S = \emptyset$. The other three cases are considered below.

k	Eq. 6	exist	Thm. 7 & 9	$S = -S$	$S = tS$	Cor. 15
3	1		1			
4	2		2			
5	2		2			
6	5	1	4			
7	5	1	3			
8	10		4	2	3	
9	13		8	3	1	
10	15		7	1	4	1
11	11		8	1	2	
12	27	2	11	7	4	2
13	17	1	10	1	4	
14	22		12		8	
15	42	2	29	4	7	

First we need a lemma about homomorphic image of S on a factorgroup of G.

Lemma 14 *Suppose that Cay(G, S) is an NRD(v, k, λ, μ) and suppose that H is a normal subgroup of G of order u. Let $v = uw$. Then there is a $w \times w$ matrix M with integer entries so that*

$$MM^T = \eta I_w + \mu u J_w$$

If $\mu > \lambda$ then the entries are non-negative. Otherwise there may be one negative entry in each row.

The sum of all enties in any row or column is ρ.

Proof Let P denote the natural homomorphism $G \mapsto G/H$ and its extention to the group rings. From the equation

$$\pi\pi^{[-1]} = \mu\gamma + \eta$$

we get by applying P:

$$P(\pi)P(\pi^{[-1]}) = \mu u\phi + \eta$$

where $\phi = \sum_{x\in G/H} x$. Let $P(\pi) = \sum a_x x$. Then $P(\pi^{[-1]}) = \sum a_x x^{-1}$. Thus

$$\sum_{x,y} a_x a_y xy^{-1} = \mu u\phi + \eta$$

and so

$$\sum_z (\sum_x a_x a_{z^{-1}x})z = \mu u \sum_z z + \eta$$

From this we get

$$\begin{array}{l} \sum_x a_x a_{z^{-1}x} = \mu u, \quad z \neq 1 \\ \sum_x a_x^2 = \mu u + \eta, \quad z = 1 \end{array} \tag{20}$$

Define a $w \times w$ matrix M with rows and column indexed by the elements of G/H so that $M_{x,y} = a_{xy}$.

In order to calculate MM^T we get from equation 20

$$\sum_y a_{xy}a_{x'y} = \begin{cases} \mu u + \eta & x = x' \\ \mu u & x \neq x' \end{cases}$$

from which the result follows. ◇

Corollary 15 *Suppose that there an NRD(v, k, λ, μ) which is a Cayley graph of an abelian group. Let u divide v. Then*
$x^2 = \eta y^2 + \mu u z^2$ *has a non-trivial integer solution if* $\frac{v}{u} \equiv 1 \mod 4$
$x^2 = \eta y^2 - \mu u z^2$ *has a non-trivial integer solution if* $\frac{v}{u} \equiv 3 \mod 4$

Proof As there is a subgroup of order u, the result follows immediately from the Lemma 14 and Lemma 8. ◇

Example Let $(v, k, \lambda, \mu) = (120, 14, 0, 2)$ and suppose that there is a cyclic NRD with these parameters. Then $\eta = \rho = 16$.

Take $u = 30$ in the lemma. Then we get a 4×4 matrix M with non-negative entries. The set of enties in any row has sum 16 and square-sum 76. The only possible sets are

$$\{7, 3, 3, 3\} \text{ and } \{5, 5, 5, 1\}.$$

With $u = 15$ the possible sets of entries in a row is

$$\{5, 3, 2, 2, 1, 1, 1, 1\}$$

$$\{5, 2, 2, 2, 2, 2, 1, 0\}$$

$$\{4, 4, 3, 1, 1, 1, 1, 1\}$$

$$\{4, 4, 2, 2, 2, 1, 1, 0\}$$

$$\{4, 3, 3, 3, 1, 1, 1, 0\}$$

$$\{4, 3, 3, 2, 2, 2, 0, 0\}$$

$$\{3, 3, 3, 3, 3, 1, 0, 0\}$$

For any such set that comes from the above lemma, it should be possible to pair the elements in such a way that the set of sums of pairs is one of the two sets for $u = 30$. For each of the seven sets listed it can be seen that this is not possible. Thus the graph does not exist. $\diamond$

Example Let $(v, k, \lambda, \mu) = (55, 12, 3, 2)$ and suppose that there is cyclic NRD, $\mathrm{Cay}(\mathbb{Z}_{55}, \mathbb{S})$ with these parameters. Then $\eta = \rho = 11$.

Take $u = 5$ in the lemma. Then we get an 11×11 matrix M. The entries in a row are all non-negative integers except possibly one which may be -1. The sum of entries in a row is 11 and square-sum is 21. In can be checked that the set of entries in a row is one of the following four possibilities:

$$\{3, 2, 2, 1, 1, 1, 1, 0, 0, 0, 0\}$$

$$\{2, 2, 2, 2, 2, 1, 0, 0, 0, 0, 0\}$$

$$\{-1, 3, 2, 1, 1, 1, 1, 1, 1, 1, 0\}$$

$$\{-1, 2, 2, 2, 2, 1, 1, 1, 1, 0, 0\}$$

As M is back-circulant we see by investigating all permutations of the elements in these sets that M must contain one of the following vectors as a row (so there 22 possibilities for M)

$$(2, 2, 2, 0, 2, 1, 0, 2, 0, 0, 0)$$

$$(0, 0, 0, 2, 0, 1, 2, 0, 2, 2, 2)$$

If the first row of the matrix is $(a_0, \ldots, a_{10})$, it means that the coset

$$\{0, 11, 22, 33, 44\} + 11i$$

contains a_i elements of S, if $i \neq 0$ and $a_0 + 1$ for $i = 0$. As $S \cap -S = \emptyset$ we see that $a_0 \leq 1$. Thus there are only 12 possibilities for M. Each of these can be checked by computersearch. The result is that the graph does not exist. $\diamond$

Example Let $(v, k, \lambda, \mu) = (64, 14, 4, 2)$ and suppose that there is a cyclic NRD, $\mathrm{Cay}(\mathbb{Z}_{\not\vartriangleleft\not\trianglerighteq}, \mathbb{S})$ with these parameters. Then $\eta = 16, \rho = 12$.

Take $u = 4$ in the lemma. Then we get a 16×16 matrix M. Let $(a_0, \ldots, a_{15})$ be the first row of this matrix. Then $\sum a_i = 12, \sum a_i^2 = 24$ and $a_i \geq 0$ for $i \geq 1$. As $S \cap \{0, 16, 32, 48\}$ has at most one element, $a_0 = -2$ or -1. Similarly, $a_8 \leq 2$. As in the above example we see (by computersearch) that the first row of M is one of the following

$$(-2, 2, 1, 1, 0, 0, 1, 1, 2, 2, 1, 1, 0, 0, 1, 1)$$

$$(-2, 1, 2, 1, 0, 1, 0, 1, 2, 1, 2, 1, 0, 1, 0, 1)$$

$$(-2, 1, 1, 2, 0, 1, 1, 0, 2, 1, 1, 2, 0, 1, 1, 0)$$

$$(-2, 1, 1, 0, 2, 1, 1, 0, 2, 1, 1, 0, 2, 1, 1, 0)$$

$$(-2, 1, 1, 0, 0, 1, 1, 2, 2, 1, 1, 0, 0, 1, 1, 2)$$

$$(-2, 1, 0, 1, 2, 1, 0, 1, 2, 1, 0, 1, 2, 1, 0, 1)$$
$$(-2, 1, 0, 1, 0, 1, 2, 1, 2, 1, 0, 1, 0, 1, 2, 1)$$
$$(-2, 0, 1, 1, 2, 0, 1, 1, 2, 0, 1, 1, 2, 0, 1, 1)$$
$$(-2, 0, 1, 1, 0, 2, 1, 1, 2, 0, 1, 1, 0, 2, 1, 1)$$

As the elements of S cannot all be multiples of 2, some element of S is relatively prime to 64. By applying some group automorphism we may assume that $1 \in S$. So in fact the last two possibilities for the first of M need not be investigated. Now a computersearch shows that the graph does not exist. $\diamond$

4.3 Cayley digraphs from non-cyclic groups

Until now we have mainly looked at Cayley digraphs from cyclic groups. Only in the construction in Theorem 12 the group need not be cyclic. Another example is the following.

Example The digraph Cay($\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3, S$) is an NRD(27,10,3,5), where S denotes the set

$$S = \{(1,0,0),(0,1,0),(0,0,1),(1,1,0),(1,0,1),(0,1,1),\\ (1,1,2),(1,2,1),(2,1,1),(2,2,2)\}.$$

For every $s = 2^n$, Liebler and Mena [12] has constructed a distance regular digraph of girth 4 and degree $s(2s^2-1)$, as a Cayley digraph of $\mathbb{Z}_4 \times \ldots \times \mathbb{Z}_4$. Their graph is in fact an NRD$(4s^4, s(2s^2-1), 2s(s-1), s(s-1))$.

References

[1] T. Beth, D. Jungnickel and H. Lenz, Design Theory, Bibliographisches Institut (1985) and Cambridge University Press (1993).

[2] R. M. Damerell, Distance-transitive and distance-regular digraphs, *J. Combin. Th. B* **31** (1981) 46–53.

[3] A. M. Duval, A Directed Version of Strongly Regular Graphs, *J. Combin. Th. (A)* **47** (1972) 71–100

[4] E. Fried and V. Sós, Weakly associative lattices and projective planes, *Algebra Universalis* **5** (1975) 114–119.

[5] M. Hall, Jr., Combinatorial Theory, second edition, Wiley-Interscience (1986).

[6] P. Hall, On representatives of subsets, *J. London Math. Soc* **10** (1935) 26–30.

[7] N. Ito, Doubly regular asymmetric digraphs, *Discr. Math.* **72** (1988) 181–185.

[8] N. Ito, On Hadamard Tournaments, *J. Algebra* **131** (1990) 432–443.

[9] L. K. Jørgensen, Bipartite graphs with small diameter and defect 2.

[10] L. K. Jørgensen, Isomorphic switching in tournaments, Technical Report R-94-2021, Institute for Electronic Systems, Aalborg University.

[11] A. Kotzig, Sur les tournois avec des 3-cycles régulière-ment placés, *Mat. Casopis* **19** (1969) 126–134.

[12] R. A. Liebler and R. A. Mena, Certain distance-regular digraphs and related rings of characteristic 4, *J. Combin. Th. (A)* **47** (1988) 111–123.

[13] K. B. Reid and E. Brown, Doubly Regular Tournaments are Equivalent to Skew Hadamard Matrices, *J. Combin. Th. (A)* **12** (1988) 332–338.

[14] P. Rowlinson, On 4-cycles and 5-cycles in regular tournaments, *Bull. London Math. Soc.* **18** (1986) 135–139.

[15] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938) 377–385.

[16] A. Torgaśev, The spectrum of a normal digraph, *Univ. Novi Sad, Coll. of papers Fac. Sci. (Ser. Math.)* **17,1** (1987) 187–200.