NEW ZEALAND JOURNAL OF MATHEMATICS
Volume 33 (2004), 113–119

DIRECTED GRAPHS AND MINIMUM DISTANCES OF ERROR–CORRECTING CODES IN MATRIX RINGS

Sergey Bereg, Andrei Kelarev, and Ana Sălăgean

(Received May 2002)

Abstract. The main theorems of this paper give sharp upper bounds for the minimum distances of one-sided ideals in structural matrix rings defined by directed graphs.

It is very well known that additional algebraic structure can give advantages for coding applications (see, for example, [**8**]). Serious attention in the literature has been devoted to considering properties of ideals in various ring constructions essential from the point of view of coding theory (see the survey [**7**] and books [**4**], [**9**], [**10**]). The investigation of code properties of ideals in structural matrix rings of directed graphs was begun in [**6**], where two-sided ideals are considered. The aim of this paper is to strengthen the results of [**6**] and obtain sharp upper bounds for the minimum distances of one–sided ideals in structural matrix rings defined by directed graphs.

Let F be a finite field. Throughout, the word *graph* means a directed graph without multiple edges but possibly with loops, and $D = (V, E)$ stands for a graph with the set $V = \{1, 2, \dots, n\}$ of vertices and the set E of edges. Edges of D correspond to the standard elementary matrices of the algebra $M_n(F)$ of all $(n \times n)$–matrices over F. Namely, for $(i, j) \in E \subseteq V \times V$, let $e_{(i,j)} = e_{i,j} = e_{ij}$ be the standard elementary matrix. Note that

$$e_{i,j}e_{k,l} = \begin{cases} 0 & \text{if } \; j \neq k, \\ e_{i,l} & \text{if } \; j = k. \end{cases}$$

Denote by

$$M_D(F) = \bigoplus_{w \in E} F e_w$$

the set of all matrices with arbitrary entries from F corresponding to the edges of the graph D, and zeros in all entries for which there are no edges in D. It is known and easy to verify that $M_D(F)$ is a subalgebra of $M_n(F)$ if and only if D satisfies the following property

$$(x, y), (y, z) \in E \Rightarrow (x, z) \in E, \tag{1}$$

for all $x, y, z \in V$. In this case $M_D(F)$ is called a *structural matrix ring*. Many interesting results on structural matrix rings have been obtained in the literature (see, for example, [**2**], [**3**], [**11**], [**12**], [**13**]). Known facts and references concerning structural matrix rings can be also found in the monograph [**4**].

2000 *AMS Mathematics Subject Classification:* 94B05, 94B15, 94B25.
The second author has been supported by ARC Discovery grant DP0449469.

If $x, y \in V$, then a *directed path* from x to y is a sequence of vertices $x = x_0, x_1, \ldots, x_m = y$ such that $m \geq 1$ and $(x_i, x_{i+1}) \in E$ for $i = 0, \ldots, m-1$. Property (1) is equivalent to the following:

$$\text{if there is a directed path from } \; x \; \text{ to } \; z, \; \text{ then } \; (x, z) \in E, \tag{2}$$

for all $x, z \in V$. Both (1) and (2) are equivalent to the relation E being transitive.

Recall that the *in–degree* and *out–degree* of a vertex $v \in V$ are defined by

$$\operatorname{indeg}(v) = \operatorname{indeg}_D(v) = |\{w \in V \mid (w, v) \in E\}|,$$
$$\operatorname{outdeg}(v) = \operatorname{outdeg}_D(v) = |\{w \in V \mid (v, w) \in E\}|.$$

A vertex of D is called a *source* (*sink*) if $\operatorname{indeg}(v) = 0$ and $\operatorname{outdeg}(v) > 0$ (respectively, $\operatorname{indeg}(v) > 0$, $\operatorname{outdeg}(v) = 0$). Denote by $\operatorname{so}(D)$ and $\operatorname{si}(D)$ the sets of all sources and sinks of D, respectively. For each vertex $v \in V$, put

$$\operatorname{so}(v) = \operatorname{so}_D(v) = \{u \in \operatorname{so}(D) \mid (u, v) \in E\},$$
$$\operatorname{si}(v) = \operatorname{si}_D(v) = \{u \in \operatorname{si}(D) \mid (v, u) \in E\}.$$

Note that in a graph satisfying property (1) we have, using (2) that

$$\operatorname{so}(v) = \{u \in \operatorname{so}(D) \mid \text{there is a directed path from } u \text{ to } v\},$$
$$\operatorname{si}(v) = \{u \in \operatorname{si}(D) \mid \text{there is a directed path from } v \text{ to } u\}.$$

We use standard concepts of coding theory following [**9**] (see also [**10**] and [**5**], Chapter 2). The minimum distance is worth considering from the point of view of coding theory, because it gives the number of errors a code can detect or correct. Denote by $\operatorname{wt}(x)$ the Hamming weight of an element $x \in M_n(F)$, i.e., the number of nonzero entries of the matrix x. The Hamming distance between two elements and the minimum distance of a code are then defined in the usual way. The distance between two elements is the weight of their difference. The minimum distance $\operatorname{d}(C)$ of a code C is the minimum distance between a pair of distinct elements in the code. If a code is a linear space, then its minimum distance is equal to the minimum weight of a nonzero element in the code.

We will be interested in codes that are one–sided ideals in $M_D(F)$. The left (right) ideal generated by an element $x \in M_D(F)$ will be denoted by $\operatorname{id}_\ell(x)$ $\big(\operatorname{id}_r(x)$ respectively$\big)$. Denote by $\operatorname{d}_\ell(D)$ $\big($and $\operatorname{d}_r(D)\big)$ the maximum among the distances of all left (resp., right) ideals of the ring $M_D(F)$, i.e.,

$$\operatorname{d}_\ell(D) \;=\; \max\{\operatorname{d}(I) \mid I \text{ left ideal in } \; M_D(F)\}.$$

Theorem 1. *Let $D = (V, E)$ be a graph defining a structural matrix ring $M_D(F)$. Then:*

$$\operatorname{d}_\ell(D) \;=\; \max\left\{\max_{v \in V} \operatorname{outdeg}(v), \quad \sum_{v \in \operatorname{so}(D)} \operatorname{outdeg}(v)\right\}. \tag{3}$$

Proof. Denote by $L(D)$ the quantity in the right hand side of (3), i.e.,

$$L(D) \;=\; \max\left\{\max_{v \in V} \operatorname{outdeg}(v), \quad \sum_{v \in \operatorname{so}(D)} \operatorname{outdeg}(v)\right\}.$$

We prove first that $\operatorname{d}_\ell(D) \geq L(D)$ by showing that $M_D(F)$ always has a left ideal with minimum distance $L(D)$.

Assume first that $\sum_{v\in \mathrm{so}(D)} \mathrm{outdeg}(v) \geq \max_{v\in V} \mathrm{outdeg}(v)$. This obviously implies that D has sources. Denote by S the set of edges originating at a source, i.e., $S = E \cap \big(\mathrm{so}(D) \times V\big)$. Let $x = \sum_{(u,v)\in S} e_{u,v}$ and let $I = \mathrm{id}_\ell(x)$. Obviously, $\mathrm{wt}(x) = |S| = \sum_{v\in \mathrm{so}(D)} \mathrm{outdeg}(v)$. For any $(i,j) \in E$ we have $e_{i,j}x = 0$, as j cannot be a source . Hence $I = Fx$ and $\mathrm{d}(I) = \mathrm{wt}(x) = \sum_{v\in \mathrm{so}(D)} \mathrm{outdeg}(v) = L(D)$.

Now assume that $\sum_{v\in \mathrm{so}(D)} \mathrm{outdeg}(v) < \max_{v\in V} \mathrm{outdeg}(v)$. This means that the vertex (or vertices) with maximum out–degree in D are not sources. Let $u \in V$ be such that $\mathrm{outdeg}(u) = \max_{v\in V} \mathrm{outdeg} v$. Put $x = \sum_{(u,v)\in E} e_{u,v}$ and and $I = \mathrm{id}_\ell(x)$. Obviously $\mathrm{wt}(x) = \mathrm{outdeg}(u) = \max_{v\in V} \mathrm{outdeg} v = L(D)$. Consider an arbitrary nonzero element $y \in I$. We claim that $\mathrm{wt}(y) \geq \mathrm{wt}(x)$.

Since $I = Fx+M_D(F)x$, y is of the form $y = fx+ax$ with $f \in F$ and $a \in M_D(F)$. Writing a as $a = \sum_{(i,j)\in E} a_{i,j}e_{i,j}$, where $a_{i,j} \in F$, we get

$$y \ = \ fx + \sum_{(i,u)\in E} a_{i,u} \sum_{(u,v)\in E} e_{i,v}. \tag{4}$$

We may assume that (4) has been simplified by combining similar terms, i.e., terms with equal edges. If $(u,u) \in E$, then $a_{u,u}e_{u,u}x = a_{u,u}x$ and this product can be combined with fx. Therefore we may assume that $a_{u,u} = 0$. The remaining summands in ax do not result in edges beginning at u. It follows that if $f \neq 0$, then $\mathrm{wt}(y) \geq \mathrm{wt}(fx) = \mathrm{wt}(x)$, as required. Assume now $f = 0$. Since $y = ax \neq 0$, clearly there exists $j \in V$ such that $(j,u) \in E$ and $a_{j,u} \neq 0$. Therefore

$$\mathrm{wt}(y) = \mathrm{wt}\left(\sum_{(i,u)\in E} a_{i,u} \sum_{(u,v)\in E} e_{i,v}\right) \geq \mathrm{wt}(a_{j,u} \sum_{(u,v)\in E} e_{j,v}) = \mathrm{wt}(a_{j,u}e_{j,u}x) = \mathrm{wt}(x)$$

and so $\mathrm{d}(I) = \mathrm{wt}(x) = \max_{v\in V} \mathrm{outdeg} v = L(D)$ as required. This concludes the proof of the inequality $\mathrm{d}_\ell(D) \geq L(D)$.

Next we will show that any left ideal I of $M_D(F)$ has minimum distance less than or equal to the $L(D)$, thus proving that $\mathrm{d}_\ell(D) \leq L(D)$. Let $x \in I$ be such that $\mathrm{d}(I) = \mathrm{wt}(x)$. Write x as $x = \sum_{(i,j)\in E} x_{i,j}e_{i,j}$.

We consider first the case when all vertices i with $x_{i,j} \neq 0$ are sources. Then $\{(i,j) \mid x_{ij} \neq 0\} \subseteq S$, so $\mathrm{wt}(x) \leq \sum_{v\in \mathrm{so}(D)} \mathrm{outdeg}(v) \leq L(D)$.

Next we consider the case when there is at least a $x_{uw} \neq 0$ with u not a source. Since u is not a source, there is $u_1 \in V$ with $(u_1,u) \in E$. Let $y = e_{u_1u}x \in I$. We have:

$$y = e_{u_1u}x = \sum_{(u,j)\in E} x_{uj}e_{u_1,j}.$$

Then $y \neq 0$, $y \in I$ and $\mathrm{wt}(y) \leq \mathrm{wt}(x)$. By the minimality of $\mathrm{wt}(x)$ we infer $\mathrm{wt}(x) = \mathrm{wt}(y)$. On the other hand, $\mathrm{wt}(y) \leq \mathrm{outdeg}(u) \leq \max_{v\in V} \mathrm{outdeg} v$. Hence $\mathrm{wt}(x) \leq \max_{v\in V} \mathrm{outdeg} v \leq L(D)$, which completes our proof. □

Corollary 2. *In the conditions of Theorem 1, we have*

$$\mathit{distl}(D) \ = \ \max\left\{ \max_{\substack{v\in V\setminus \mathrm{so}(D),\\ \mathrm{so}(v)=\varnothing}} \mathrm{outdeg}(v), \quad \sum_{v\in \mathrm{so}(D)} \mathrm{outdeg}(v) \right\}. \tag{5}$$

Proof. In view of the result given by (3), all we have to prove is that when the inequality

$$\max_{v\in V} \operatorname{outdeg}(v) \; > \sum_{v\in \operatorname{so}(D)} \operatorname{outdeg}(v) \tag{6}$$

holds, then it follows that

$$\max_{v\in V} \operatorname{outdeg}(v) \; = \max_{\substack{v\in V\setminus \operatorname{so}(D),\\ \operatorname{so}(v)=\varnothing}} \operatorname{outdeg}(v).$$

Assume therefore that (6) holds and let $u \in V$ be such that $\operatorname{outdeg}(u) = \max_{v\in V} \operatorname{outdeg}(v)$. It suffices to show that $u \in V \setminus \operatorname{so}(D)$ and $\operatorname{so}(u) = \varnothing$.

If $u \in \operatorname{so}(D)$ then $\operatorname{outdeg}(u) \le \sum_{v\in \operatorname{so}(D)} \operatorname{outdeg}(v)$ contradicting (6). We show now that $\operatorname{so}(u) = \varnothing$. Assume that $\operatorname{so}(u) \neq \varnothing$. Then there is a vertex $w \in \operatorname{so}(D)$ such that $(w, u) \in E$. For any $(u, v) \in E$ we have that $(w, v) \in E$, by property (1). Hence $\operatorname{outdeg}(w) \ge \operatorname{outdeg}(u)$. The maximality of $\operatorname{outdeg}(u)$ implies that $\operatorname{outdeg}(w) = \operatorname{outdeg}(u) = \max_{v\in V} \operatorname{outdeg}(v)$. But w is a source, so $\operatorname{outdeg}(w) \le \sum_{v\in \operatorname{so}(D)} \operatorname{outdeg}(v)$ contradicting (6). Hence we proved that $u \in V \setminus \operatorname{so}(D)$ and $\operatorname{so}(u) = \varnothing$, as required. □

Remark 3. Every structural matrix ring can be thought of as a semigroup ring. Let S be a finite semigroup. Recall that the *semigroup ring* $F[S]$ consists of all sums of the form $\sum_{s\in S} r_s s$, where $r_s \in F$ for all $s \in S$, with addition and multiplication defined by the rules

$$\sum_{s\in S} r_s s + \sum_{s\in S} r'_s s \; = \; \sum_{s\in S} (r_s + r'_s)s,$$

$$\left(\sum_{s\in S} r_s s\right)\left(\sum_{t\in S} r'_t t\right) \; = \; \sum_{s,t\in S} (r_s r'_t) st.$$

If S is a semigroup with zero θ, then the *contracted semigroup ring* $F_0[S]$ is the quotient ring of $F[S]$ modulo the ideal $F\theta$. Thus $F_0[S]$ consists of all sums of the form $\sum_{\theta\neq s\in S} r_s s$, and all elements of $F\theta$ are identified with zero.

A graph $D = (V, E)$ defines a structural matrix ring if and only if the set

$$S_D \; = \; \{\theta\} \cup \{e_{ij} \mid (i, j) \in E\}$$

forms a semigroup, and both of these properties are equivalent to condition (1). Then it is easily seen that the structural matrix ring $M_D(F)$ is isomorphic to the contracted semigroup ring $F_0[S_D]$. Thus our note also continues the investigation of coding properties of ideals in semigroup rings started in [**1**].

We now move to the case of right ideals. Analogues of Theorem 1 and Corollary 2, with outdeg replaced by indeg and sources replaces by sinks, can be proven in a similar way. Alternatively, such results can be deduced from Theorem 1 and Corollary 2 using the notion of a *reversed graph*. Namely, given a graph $D = (V, E)$, its reversed graph is $D^{-1} = (V, E^{-1})$, where $E^{-1} = \{(u, v) \mid (v, u) \in E\}$.

Lemma 4. *Let $D = (V, E)$ be a graph defining a structural matrix ring $M_D(F)$. Then the reversed graph $D^{-1} = (V, E^{-1})$ defines a structural matrix ring that is* *antiisomorphic to the structural matrix ring $M_{D^{-1}}(F)$ with the antiisomorphism given by*

$$\sum_{(u,v)\in E} r_{(u,v)} e_{(u,v)} \ \mapsto \ \sum_{(v,u)\in E^{-1}} r_{(u,v)} e_{(v,u)}. \tag{7}$$

Proof is straightforward and we omit it. Combining Lemma 4 with Theorem 1 and Corollary 2, we get the following formulas for the largest minimum distance of right ideals in the ring $M_D(F)$.

Theorem 5. *Let $D = (V, E)$ be a graph defining a structural matrix ring $M_D(F)$. Then:*

$$\mathrm{d}_r(D) \ = \ \max\left\{ \sum_{v\in \mathrm{si}(D)} \mathrm{indeg}(v), \quad \max_{v\in V} \mathrm{indeg}(v) \right\}. \tag{8}$$

Corollary 6. *In the conditions of Theorem* 1*, we have*

$$\mathrm{d}_r(D) \ = \ \max\left\{ \max_{\substack{v\in V\setminus \mathrm{si}(D),\\ \mathrm{si}(v)=\varnothing}} \mathrm{indeg}(v), \quad \sum_{v\in \mathrm{si}(D)} \mathrm{indeg}(v) \right\}. \tag{9}$$

Proof. Let $D^{-1} = (V, E^{-1})$ be the reversed graph of $D = (V, E)$. From the definition of the reversed graph we obtain the following equalities:

$$\begin{aligned} \mathrm{si}(D) &= \mathrm{so}(D^{-1}), \\ \mathrm{indeg}_D(v) &= \mathrm{outdeg}_{D^{-1}}(v). \end{aligned}$$

Therefore it follows that

$$\max_{v\in W_1} \mathrm{indeg}_D(v) \ = \ \max_{v\in W_2} \mathrm{outdeg}_{D^{-1}}(v),$$

where

$$W_1 = \{v \in V \mid v \notin \mathrm{si}(D),\ \mathrm{si}(v) = \varnothing\}$$

and

$$W_2 = \{v \in V \mid v \notin \mathrm{so}(D^{-1}),\ \mathrm{so}(v) = \varnothing\}.$$

Besides,

$$\sum_{v\in \mathrm{si}(D)} \mathrm{indeg}_D(v) \ = \ \sum_{v\in \mathrm{so}(D^{-1})} \mathrm{outdeg}_{D^{-1}}(v).$$

When we consider the minimum distance $\mathrm{d}(C)$ of a linear code C regarded as a subspace of a linear space L, the distance is defined with respect to a certain fixed basis B of the whole linear space L, and so we may use the notation $\mathrm{d}_B(C)$ to emphasize this. Note that if $f : V_1 \to V_2$ is an isomorphism or an antiisomorphism of two linear spaces V_1 and V_2 such that f maps the basis B_1 of V_1 to the basis B_2 of V_2, then for every linear code C in V_1 we have

$$\mathrm{d}_{B_1}(C) \ = \ \mathrm{d}_{B_2}\big(f(C)\big). \tag{10}$$

Clearly, the antiisomorphism defined by (7) maps the basis

$$B_1 \ = \ \{e_{i,j} \mid (i,j) \in E\}$$

of $M_D(F)$, used in the definition of the minimum distance, onto the corresponding basis

$$B_2 \;=\; \{e_{j,i} \mid (j,i) \in E^{-1}\}$$

of $M_{D^{-1}}(F)$. Lemma 4 implies therefore

$$\mathrm{d}_r(D) \;=\; \mathrm{d}_\ell(D^{-1})$$

Hence it follows that (3) and (5) yield (8) and (9), respectively. □

The authors are grateful to the referee for corrections that have improved our text.

References

1. J. Cazaran and A.V. Kelarev, *Generators and weights of polynomial codes*, Arch. Math. (Basel) **69** (1997), 479–486.
2. S. Dăscălescu and L. van Wyk, *Do isomorphic structural matrix rings have isomorphic graphs?*, Proc. Amer. Math. Soc. **124** (1996), 1385–1391.
3. B.W. Green and L. van Wyk, *On the small and essential ideals in certain classes of rings*, J. Austral. Math. Soc. Ser. A **46** (1989), 262–271.
4. A.V. Kelarev, *Ring Constructions and Applications*, World Scientific, 2002.
5. A.V. Kelarev, *Graph Algebras and Automata*, Marcel Dekker, 2003.
6. A.V. Kelarev and O.V. Sokratova, *Information rates and weights of codes in structural matrix rings*, 14th International Symposium, AAECC–14, Melbourne, Australia, November 2001, Lecture Notes Computer Science, **2227** (2001), 151–158.
7. A.V. Kelarev and P. Sole, *Error–correcting codes as ideals in group ring*, Contemporary Mathematics, **273** (2001), 11–18.
8. R. Lidl and G. Pilz, *Applied Abstract Algebra*, Springer–Verlag, New York, 1998.
9. V.S. Pless, W.C. Huffman and R.A. Brualdi, *Handbook of Coding Theory*, Elsevier, New York, 1998.
10. A. Poli and L. Huguet, *Error-Correcting Codes: Theory and Applications*, Prentice–Hall, 1992.
11. L. van Wyk, *Matrix rings satisfying column sum conditions versus structural matrix rings*, Linear Algebra Appl. **249** (1996), 15–28.
12. L. van Wyk, *A link between a natural centralizer and the smallest essential ideal in structural matrix rings*, Comm. Algebra, **27** (1999), 3675–3683.

13. S. Veldsman, *On the radicals of structural matrix rings*, Monatsh. Math. **122** (1996), 227–238.

Sergey Bereg
Department of Computer Science
University of Texas at Dallas
Box 830688
Richardson TX 75083
USA
besp@utdallas.edu

Andrei Kelarev
School of Computing, University of Tasmania
Private Bag 100
Hobart
Tasmania 7001
AUSTRALIA
Andrei.Kelarev@utas.edu.au

Department of Computer Science
Loughborough University
Loughborough LE11 3TU
United Kingdom
A.M.Salagean@lboro.ac.uk