IJMMS 2003:13, 827–833
PII. S0161171203204063
http://ijmms.hindawi.com

MINIMUM DISTANCES OF ERROR-CORRECTING CODES IN INCIDENCE RINGS

A. V. KELAREV

Received 7 April 2002

The main theorem of this paper gives a formula for the largest minimum distance of error-correcting codes considered as ideals in incidence rings defined by directed graphs.

2000 Mathematics Subject Classification: 94B60, 94B65, 16S50.

It is very well known that additional algebraic structure can give advantages for coding applications. For example, all cyclic error-correcting codes are principal ideals in the group algebras of cyclic groups (see the survey [4] and the books [3, 5, 6, 7]). 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. The aim of this paper is to obtain a formula for the largest minimum distance of ideals in incidence rings defined by directed graphs.

Let R be a ring with identity element 1, and let $D = (V,E)$ be any graph with the set $V = \{1,\dots,n\}$ of vertices and a set $E \subseteq V \times V$ of edges. We use the standard definition of an incidence ring (see, e.g., [3, Section 3.15]). The *incidence ring* $I(D,R)$ is the free left R-module with basis consisting of all edges in E, where multiplication is defined by the distributive law and the rule

$$(x,y)\cdot(z,w) = \begin{cases} (x,w), & \text{if } y = z,\ (x,w) \in E, \\ 0, & \text{otherwise,} \end{cases} \tag{1}$$

for all $x,y,x,t \in V$. The graph D is said to be *balanced* if for all $x_1,x_2,x_3,x_4 \in V$ with $(x_1,x_2),(x_2,x_3),(x_3,x_4),(x_1,x_4) \in E$,

$$(x_1,x_3) \in E \iff (x_2,x_4) \in E. \tag{2}$$

It is proved in [1] that $I(D,R)$ is an associative ring if and only if D is balanced.

For any vertex $v \in V$, we introduce the following sets of vertices:

$$\begin{aligned} \mathrm{In}(v) &= \mathrm{In}_D(v) = \{x \in V \mid (x,v) \in E\}, \\ \mathrm{Out}(v) &= \mathrm{Out}_D(v) = \{x \in V \mid (v,x) \in E\}. \end{aligned} \tag{3}$$

Denote by E_{down} the set of all edges $(x,y) \in E$ such that there exists $z \in V$ with $(z,x),(z,y) \in E$. Let E_{up} be the set of all edges $(x,y) \in E$ such that there exists $z \in V$ with $(x,z),(y,z) \in E$. Put $E_0 = E \setminus (E_{\text{up}} \cup E_{\text{down}})$.

For each vertex $v \in V$ and a subset $S \subseteq \text{Out}(v)$, denote by $\text{In}^S(v)$ the set of all $x \in V$ such that the following conditions hold:

(I1) $(x,v) \in E \setminus E_{\text{down}}$;

(I2) for every $y \in \text{Out}(v)$, $(x,y) \in E$ if and only if $y \in S$.

Similarly, for each $S \subseteq \text{In}(v)$, denote by $\text{Out}^S(v)$ the set of all $y \in V$ such that the following conditions hold:

(O1) $(v,y) \in E \setminus E_{\text{up}}$;

(O2) for every $x \in \text{In}(v)$, $(x,y) \in E$ if and only if $x \in S$.

The minimum distance is worth considering from the viewpoint of coding theory, because it gives the number of errors a code can detect or correct. Denote by $\text{wt}(x)$ the Hamming weight of an element $x \in M_n(F)$, that is, the number of edges (u_i,v_i) with nonzero coefficients r_i in the standard record $x = \sum_{i=1}^{n} r_i(u_i,v_i)$. 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 Hamming weight of their difference. The minimum distance $\text{dist}(C)$ 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. An ideal is said to be *principal* if it is generated by one element. This property is also convenient since, in order to store the whole code in computer memory, it is enough to record only one generator. Besides, the generators of codes are used in encoding and decoding algorithms. This is why it is nice that the best minimum distances for all ideals in incidence rings are achieved by principal ideals, as the following main theorem shows. We do not assume that all vertices of the graph have loops since, otherwise, all ideals of the incidence ring have minimum distance one, and being regarded as codes they cannot detect even one error.

Theorem 1. *Let $D = (V,E)$ be a balanced graph, and let R be a ring with identity element. Then the incidence ring $I(D,R)$ has a principal ideal with minimum distance*

$$\text{dist}(D) = \max\left\{1, |E_0|, \max_{v \in V, S \subseteq \text{Out}(v)} |\text{In}^S(v)|, \max_{v \in V, S \subseteq \text{In}(v)} |\text{Out}^S(v)|\right\} \tag{4}$$

and the minimum distances of all ideals of $I(R,D)$ do not exceed $\text{dist}(D)$.

Proof. In the first part of the proof, we show that the incidence ring $I(D,R)$ always contains a principal ideal with the minimum distance given by (4).

First, consider the ideal A generated in $I(D,R)$ by the element $a = \sum_{(x,y) \in E_0}(x,y)$, where we assume that $a = 0$ if $E_0 = \varnothing$. If K is an associative ring not necessarily containing an identity element, then the left and right

annihilators of K are the sets

$$\begin{aligned} \mathrm{Ann}_\ell(K) &= \{x \in K \mid xK = 0\}, \\ \mathrm{Ann}_r(K) &= \{x \in K \mid Kx = 0\}. \end{aligned} \tag{5}$$

The annihilator of the ring K is the set defined by

$$\mathrm{Ann}(K) = \mathrm{Ann}_\ell(K) \cap \mathrm{Ann}_r(K). \tag{6}$$

The definitions of E_{up}, E_{down}, E_0, and (1) imply that the following inclusions hold:

$$E \setminus E_{\mathrm{up}} \subseteq \mathrm{Ann}_\ell\left(I(D,R)\right), \tag{7}$$

$$E \setminus E_{\mathrm{down}} \subseteq \mathrm{Ann}_r\left(I(D,R)\right), \tag{8}$$

$$E_0 \subseteq \mathrm{Ann}\left(I(D,R)\right). \tag{9}$$

It follows from (9) that the ideal A is equal to the subring generated by a. Hence, the minimum distance of A is equal to the weight of a, that is, $|E_0|$.

Second, pick any $v \in V$, $S \subseteq \mathrm{Out}(v)$, and consider the ideal $B(v,S)$ generated by $b_{v,S} = \sum_{x \in \mathrm{In}^S(v)}(x,v)$, where it is assumed that $b_{v,S} = 0$ if $\mathrm{In}^S(v) = \varnothing$. We claim that the minimum distance of $B_{v,S}$ is given by

$$\mathrm{dist}\left(B_{v,S}\right) = \mathrm{wt}\left(b_{v,S}\right) = \left|\,\mathrm{In}^S(v)\,\right|. \tag{10}$$

Indeed, each nonzero element x in the ideal $B_{v,S}$ can be written in the form

$$\begin{aligned} x = r b_{v,S} &+ \sum_{i=1}^{\ell} r_i(x_i,y_i) b_{v,S} + \sum_{j=1}^{m} r'_j b_{v,S}(z_j,w_j) \\ &+ \sum_{k=1}^{n} r''_k(u_k,v_k) b_{v,S}(e_k,f_k), \end{aligned} \tag{11}$$

where $r, r_i, r'_j, r''_k \in R$ and $x_i, y_i, z_j, w_j, u_k, v_k, e_k, f_k \in V$, for all i, j, k. The definition of $b_{v,S}$, condition (I1) and inclusion (8) show that $b_{v,S} \in \mathrm{Ann}_r(I(D,R))$. Therefore,

$$\sum_{i=1}^{\ell} r_i(x_i,y_i) b_{v,S} = \sum_{k=1}^{n} r''_k(u_k,v_k) b_{v,S}(e_k,f_k) = 0. \tag{12}$$

By the definition of $b_{v,S}$ and (1), we may remove all remaining zero summands and assume that $z_1 = \cdots = z_m = v$. Hence,

$$x = r b_{v,S} + \sum_{j=1}^{m} r'_j b_{v,S}(v,w_j). \tag{13}$$

Fix each $j \in \{1,\dots,m\}$ and every $x \in \mathrm{In}^S(v)$, condition (I2) yields that

$$(x,v)(v,w_j) \neq 0 \Longleftrightarrow w_j \in S. \tag{14}$$

Therefore, if $b_{v,S}(v,w_j) \neq 0$, then

$$\mathrm{wt}\,(b_{v,S}(v,w_j)) = \mathrm{wt}\,(b_{v,S}) = |\,\mathrm{In}^S(v)\,|. \tag{15}$$

We may assume that terms that differ only in a coefficient in R have been combined in (13). If the same edge occurs in the elements $b_{v,S}(v,w_j)$ and $b_{v,S}(v,w_k)$, then (1) implies that $w_j = w_k$, and so $b_{v,S}(v,w_j) = b_{v,S}(v,w_k)$, a contradiction. Similarly, if $b_{v,S}$ and $b_{v,S}(v,w_j)$ have a common edge, then $w_j = v$ and $b_{v,S} = b_{v,S}(v,w_j)$, a contradiction again. This establishes (10).

Third, a similar argument shows that for each $v \in V$ and $S \subseteq \mathrm{Out}(v)$, there exists an ideal with minimum distance $|\mathrm{Out}^S(v)|$. Indeed, to this end, it suffices to consider the ideal $C_{v,S}$ generated by $c_{v,S} = \sum_{x \in \mathrm{Out}^S(v)} (v,x)$, where we assume that $c_{v,S} = 0$ if $\mathrm{Out}^S(v) = 0$. A verification analogous to the one carried out in the preceding case shows that the minimum distance of $C_{v,S}$ is given by

$$\mathrm{dist}\,(C_{v,S}) = \mathrm{wt}\,(c_{v,S}) = |\,\mathrm{Out}^S(v)\,|. \tag{16}$$

Obviously, the principal ideal P generated by any element $(x,y) \in E$ has minimum distance 1. If we choose an ideal with largest minimal distance among the principal ideals P, A, $B_{v,S}$, and $C_{v,S}$, then we get the distance in (4) equal to

$$\max\left\{1, \mathrm{dist}(A), \max_{v \in V, S \subseteq \mathrm{Out}(v)} \mathrm{dist}\,(B_{v,S}), \max_{v \in V, S \subseteq \mathrm{In}(v)} \mathrm{dist}\,(C_{v,S})\,|\,\right\}. \tag{17}$$

In the second part of the proof, we take an arbitrary ideal K of $I(D,R)$ and show that the distance of K is less than or equal to the one given by (4). Choose a nonzero element $w = \sum_{i=1}^{n} r_i(x_i,y_i)$ with minimum weight in K, where $0 \neq r_i \in R$, $(x_i,y_i) \in E$, for $i = 1,\dots,n$. We have to verify that the weight n of w does not exceed the maximum in (4). Clearly, we may assume that $\mathrm{dist}(K) > 1$, and so $n > 1$.

If $(x_i,y_i) \in E_0$ for all $i = 1,\dots,n$, then $n \leq |E_0|$, and we are done. Further, assume that at least one of the edges in the expansion of w, say (x_1,y_1), is not in E_0. Then (x_1,y_1) belongs to $E_{\mathrm{down}} \cup E_{\mathrm{up}}$.

First, consider the case where $(x_1,y_1) \in E_{\mathrm{down}}$. Then, there exists $z \in V$ such that $(z,x_1),(z,y_1) \in E$. Hence, $(z,x_1)(x_1,y_1) = (z,y_1)$ and so $(z,x_1)w \neq 0$. By the minimality of the weight of w, we see that $x_1 = \cdots = x_n$ and $(z,x_1)w = \sum_{i=1}^{n} r_i(z,y_i)$. Denote by S the set of all vertices $u \in V$ such that (u,x_1), $(u,y_1) \in E$. Obviously, $S \subseteq \mathrm{In}(x_1)$. Fix any $i \in \{1,\dots,n\}$.

If $(x_1, y_i) \in E_{\mathrm{up}}$, then $(x_1, z), (y_i, z) \in E$ for some $z \in V$, and so $w(y_i, z) = r_i(x_1, z)$. By the minimality of n, we get $n = 1$, a contradiction. Hence,

$$(x_1, y_i) \in E \setminus E_{\mathrm{up}}. \tag{18}$$

Take any $x \in \mathrm{In}(x_1)$. If $(x, y_i) \in E$, then $(x, x_1)(x_1, y_i) \neq 0$, and we get that $(x, x_1)w \neq 0$, $\mathrm{wt}((x, x_1)w) = n$, $(x, x_1)(x_1, y_1) \neq 0$; whence $x \in S$. Conversely, if $x \in S$, then $(x, x_1)(x_1, y_1) \neq 0$ implies $\mathrm{wt}((x, x_1)w) = n$ and so $(x, y_i) \in E$. Thus,

$$(x, y_i) \in E \Longleftrightarrow x \in S. \tag{19}$$

Since (18) and (19) mean that conditions (O1) and (O2) are satisfied for x_1 and y_i, it follows that $y_1, \ldots, y_n \in \mathrm{Out}^S(x_1)$. Therefore, $\mathrm{wt}(w) \leq \mathrm{Out}^S(x_1)$.

Second, consider the case where $(x_1, y_1) \in E_{\mathrm{up}} \setminus E_{\mathrm{down}}$. There exist $z \in V$ such that $(x_1, z), (y_1, z) \in E$. Hence, $(x_1, y_1)(y_1, z) = (x_1, z)$, and the minimality of the weight of w implies that $y_1 = \cdots = y_n$ and $w(y_1, z) = \sum_{i=1}^{n} r_i(x_i, z)$. Now, denote by S the set of all $u \in V$ such that $(x_1, u), (y_1, u) \in E$. Clearly, $S \subseteq \mathrm{Out}(y_1)$, and it is routine to verify that, for $i = 1, \ldots, n$,

$$(x_i, y_1) \in E \setminus E_{\mathrm{down}}. \tag{20}$$

For each $y \in \mathrm{Out}(y_1)$, a similar verification shows that

$$(x_i, y) \in E \Longleftrightarrow y \in S. \tag{21}$$

By (20) and (19), conditions (I1) and (I2) are satisfied for x_i, y_1, and so $x_1, \ldots, x_n \in \mathrm{In}^S(y_1)$. Therefore, $\mathrm{wt}(w) \leq \mathrm{In}^S(y_1)$.

Thus, we see that in all possible cases, the minimum distance of the ideal K does not exceed the value in formula (4). This completes the proof. □

Our main theorem indicates that $\mathrm{dist}(D)$ is the maximum of four values. Next, we are going to give small examples showing that it is impossible to remove any of these four values from the formula. The following four graphs D_1, D_2, D_3, and D_4 are defined by their adjacency matrices A_1, A_2, A_3, and A_4, where

$$A_1 = \begin{bmatrix} 1 \end{bmatrix}, \qquad A_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

$$A_3 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}, \qquad A_4 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}. \tag{22}$$

The four values that occur in formula (4) for the graphs D_1, D_2, D_3, and D_4 are equal to $(1,0,0,0)$, $(1,2,0,0)$, $(1,0,2,0)$, and $(1,0,0,2)$, respectively.

Every incidence ring can be thought of as a *contracted semigroup ring* (see [3]). 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

$$\begin{aligned} \sum_{s\in S} r_s s + \sum_{s\in S} r'_s s &= \sum_{s\in S} (r_s + r'_s)s, \\ \left(\sum_{s\in S} r_s s\right)\left(\sum_{t\in S} r'_t t\right) &= \sum_{s,t\in S} (r_s r'_t)st. \end{aligned} \tag{23}$$

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 the sums of the form $\sum_{\theta\neq s\in S} r_s s$, and all the elements of $F\theta$ are identified with zero.

A graph $D = (V,E)$ defines an associative incidence ring if and only if the set

$$S_D = \{0\} \cup \{(i,j) \mid (i,j) \in E\} \tag{24}$$

forms a semigroup with respect to the operation defined by (1), and therefore both of these properties are equivalent to the graph being balanced. Further, it is easily seen that the incidence ring $I(D,F)$ is isomorphic to the contracted semigroup ring $F_0[S_D]$. Thus, our paper also contributes to the investigation of coding properties of ideals in semigroup rings started in [2].

Acknowledgments. The author expresses sincere appreciation to the well-known coding theory experts Professor A. A. Nechaev, for useful discussions during the AAECC1-4 conference at RMIT, Professors Kathy Horadam, Asha Baliga, Serdar Boztas, and Udaya Parampalli, for hospitality during two of his visits to the RMIT University, and to Patrick Solé for collaboration during work on our joint survey paper [4]. The author is also grateful to two referees for their helpful comments that have seriously improved this paper.

References

[1] G. Abrams, *Group gradings and recovery results for generalized incidence rings*, J. Algebra **164** (1994), no. 3, 859–876.

[2] J. Cazaran and A. V. Kelarev, *Generators and weights of polynomial codes*, Arch. Math. (Basel) **69** (1997), no. 6, 479–486.

[3] A. V. Kelarev, *Ring Constructions and Applications*, Series in Algebra, vol. 9, World Scientific Publishing, New Jersey, 2002.

[4] A. V. Kelarev and P. Solé, *Error-correcting codes as ideals in group rings*, Abelian Groups, Rings and Modules (Perth, 2000), Contemp. Math., vol. 273, American Mathematical Society, Rhode Island, 2001, pp. 11–18.

[5] R. Lidl and G. Pilz, *Applied Abstract Algebra*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1998.
[6] V. S. Pless, W. C. Huffman, and R. A. Brualdi (eds.), *Handbook of Coding Theory. Vol. I, II*, North-Holland, Amsterdam, 1998.
[7] A. Poli and L. Huguet, *Error Correcting Codes. Theory and Applications*, Prentice Hall International, Hemel Hempstead, 1992.

A. V. Kelarev: Department of Mathematics, School of Mathematics and Physics, University of Tasmania, GPO Box 252-37, Hobart, Tasmania 7001, Australia
E-mail address: andrei.kelarev@utas.edu.au