Generators and weights of polynomial codes[1]

By

Jilyana Cazaran and Andrei V. Kelarev

Introduction. Several authors have established that many classical codes are ideals in certain ring constructions. Berman [3], in the case of characteristic two, and Charpin [5], in the general case, proved that all generalized Reed-Muller codes coincide with powers of the radical of the quotient ring $A = F_q[x_1, \ldots, x_n]/(x_1^{q_1} - 1, \ldots, x_n^{q_n} - 1)$, where F_q is a finite field, $p = \operatorname{char} F_q > 0$ and $q_i = p^{c_i}$, for $i = 1, \ldots, n$, and gave formulas for their Hamming weights. These codes form an important class containing many codes of practical value. Properties of error-correcting codes in similar ring constructions A have also been considered by Poli [12].

This approach helped to improve some parameters of the codes. For example, Berman [3] showed that in certain cases abelian group codes enjoy better correcting properties than cyclic codes. Using the underlying algebraic structure, a new fast decoding algorithm for Reed-Muller codes was developed by Landrock and Manz [10].

Since the radical ideals have such good code properties, it makes sense to answer the following question: When does the radical have a single generator polynomial? Of course, if the radical is a principal ideal, then the same is obviously true of all its powers, too. Moreover, the radical of an Artinian ring is principal if and only if all ideals are principal ([1], Propositions 8.7 and 8.8). Thus the question of when the radical is a principal ideal is crucial for all other ideals to have single generator.

For example, it is well known that cyclic codes are ideals in the algebra $A = F_q[X]/(X^k - 1)$, and each ideal in A is generated by one polynomial. This property is convenient both for representing the code and for developing encoding and decoding algorithms.

Similar questions have been considered in several papers. For example, Charpin [4] described extended Reed-Solomon codes which are principal ideals.

Our first main theorem (Theorem 1) answers this question for even more general ring constructions

$$\mathbb{F}[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n)),$$

[1]This is a pre-publication version.

where $f_1, \ldots, f_n$ are arbitrary univariate polynomials and $\mathbb{F}$ is an arbitrary field. As an immediate corollary (see Corollary 3), we get the main result of [7].

A few authors have considered codes over the ring $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ of residues modulo m. A new motivation for the study of these codes has been provided recently by the results of Hammons, Kumar, Calderbank, Sloane and Solé. Namely, it is shown in [8] than many important nonlinear codes can be viewed as binary images of linear codes over $\mathbb{Z}_4$. Thus, introducing codes over $\mathbb{Z}_m$ makes it possible to apply to nonlinear codes the techniques developed earlier for linear or even polynomial codes.

Our second main theorem (Theorem 4) describes all finite ring constructions

$$\mathbb{Z}_m[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$$

whose radicals are principal ideals. It turns out that in this case the description is essentially more complicated, and does not follow from our first theorem.

After that, we give formulas for the minimum Hamming weight of the radical and its powers in the quotient ring

$$\mathbb{F}[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_n^{a_n}(1 - x_n^{b_n})).$$

1. Main theorems. If $f = g_1^{m_1} \cdots g_k^{m_k}$, where $f \in \mathbb{F}[x]$ and $g_1, \ldots, g_k$ are irreducible polynomials over $\mathbb{F}$, then by $\mathrm{sp}(f)$ we denote the squarefree part $g_1 \cdots g_k$ of f. We assume that $\mathrm{sp}(0) = 0$ and regard 0 as a squarefree polynomial. Since the Jacobson radical and nilradical $\mathcal{N}(R)$ of an Artinian ring R are identical we refer to this as the radical of R.

Theorem 1 *Let $f_1(x_1), \ldots, f_n(x_n)$ be univariate polynomials over an arbitrary field $\mathbb{F}$, and let $R = \mathbb{F}[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$. Then the radical $\mathcal{N}(R)$ is a principal ideal of R if and only if the number of polynomials $f_1, \ldots, f_n$ which are not squarefree does not exceed one.*

We shall use the following description of the radical.

Lemma 2 ([2], §8.2). *The radical of $R = \mathbb{F}[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$ is equal to the ideal generated by the squarefree parts of all polynomials $f_1, \ldots, f_n$.*

P r o o f of Theorem 1. The 'if' part immediately follows from Lemma 2. Indeed, if all $f_1, \ldots, f_n$ are squarefree, then $\mathcal{N}(R) = 0$. If f_i is not squarefree, and all the other polynomials are squarefree, then $\mathcal{N}(R)$ is generated by the squarefree part of $f_i(x_i)$.

The 'only if' part: Suppose to the contrary that the radical of R is a principal ideal, but two polynomials, say $f_1(x_1)$ and $f_2(x_2)$, are not squarefree.

Assume that $f_1, \ldots, f_k \neq 0$ and $f_{k+1}, \ldots, f_n = 0$. Then it follows from Lemma 2 that the radical $\mathcal{N}(R)$ is equal to

$$\mathcal{N}\left\{\mathbb{F}[x_1, \ldots, x_k]/(f_1(x_1), \ldots, f_k(x_k))\right\}[x_{k+1}, \ldots, x_n].$$

To simplify the notation we may assume that $k = n$, i.e. all $f_1, \ldots, f_n$ are nonzero.

Then R has finite dimension as a vector space. Therefore it is a direct sum of local rings ([1], Proposition 8.7). If the radical of a local Artinian ring is a principal ideal, then all ideals are principal by [1], Proposition 8.8. Thus R is a principal ideal ring.

Since $R/(x_3, \ldots, x_n)$ is a homomorphic image of R, it is also a principal ideal ring. Therefore we may assume that $n = 2$. Let $f_1(x_1) = g_1^{\alpha_1}(x_1) \ldots g_k^{\alpha_k}(x_1)$ where $g_1(x_1), \ldots, g_k(x_1)$ are irreducible over $\mathbb{F}$ and $\alpha_1 > 1$. Since $(g_1^{\alpha_1}, f_2) \supset (f_1, f_2)$, the ring $\mathbb{F}[x_1, x_2]/(g_1^2(x_1), f_2(x_2))$ is a homomorphic image of R and so it is a principal ideal ring too. Therefore we may assume that from the very beginning $f_1(x_1) = g_1^2(x_1)$. Given that $g_1(x_1)$ is irreducible, we see that $Q = \mathbb{F}[x_1]/(g_1(x_1))$ is a field. If we regard $f_2(x_2) \in \mathbb{F}[x_2] \subseteq Q[x_2]$ as a polynomial over Q it is not squarefree. Consider the factorization $f_2(x_2) = h_1^{\beta_1}(x_2) \ldots h_m^{\beta_m}(x_2)$ where all $h_i(x_2) \in Q[x_2]$ are irreducible and $\beta_1 > 1$. Clearly, $Q[x_2] = (\mathbb{F}[x_1]/(g_1(x_1)))[x_2] = \mathbb{F}[x_1, x_2]/(g_1(x_1))$ is a homomorphic image of $\mathbb{F}[x_1, x_2]$. Denote by $h(x_1, x_2)$ a polynomial in $\mathbb{F}[x_1, x_2]$ whose image in $Q[x_2]$ equals $h_1(x_2)$. Consider the ideal I generated by $g_1(x_1)$ and $h(x_1, x_2)$ in $\mathbb{F}[x_1, x_2]$. We see that

$$\begin{aligned} \mathbb{F}[x_1, x_2]/I &\cong \{\mathbb{F}[x_1, x_2]/(g_1(x_1))\}/\{(g_1(x_1), h(x_1, x_2))/(g_1(x_1))\} \\ &\cong Q[x_2]/h_1(x_2) \end{aligned}$$

is a field, because $h_1(x_2)$ is irreducible over Q. Therefore I is a maximal ideal. By [6], Proposition 38.4(b), the ring $\mathbb{F}[x_1, x_2]$ must not have ideals which lie strictly between I and I^2. However, $(g_1(x_1), h^2(x_1, x_2), g_1(x_1)h(x_1, x_2))$ strictly contains I^2 and is contained in I. This contradiction shows that at most one of the polynomials $f_1, \ldots, f_n$ can be squarefree. □

Theorem 1 immediately gives the main result of [7]:

Corollary 3 ([7]) *Let $\mathbb{F}$ be a field, $m \leq n$, $a_1, \ldots, a_m$ nonnegative integers, $b_1, \ldots, b_m$ positive integers, and let*

$$R = \mathbb{F}[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_m^{a_m}(1 - x_m^{b_m})).$$

If $\operatorname{char} \mathbb{F} = 0$*, then the radical of* R *is a principal ideal if and only if at most one of the* $a_1, \ldots, a_m$ *is greater than* 1*.*

If $\operatorname{char} \mathbb{F} = p > 0$*, then* R *is a principal ideal ring if and only if one of the following conditions is satisfied:*

(1) $a_1, \ldots, a_m \leq 1$ *and* p *divides at most one number among* $b_1, \ldots, b_m$*;*

(2) exactly one of $a_1, \ldots, a_m$*, say* a_1*, is greater than* 1 *and* p *does not divide each of* $b_2, \ldots, b_m$*.*

P r o o f of Corollary 3. Consider the polynomial $f = x^a(1 - x^b)$. By [2], Lemma 2.85, a polynomial is squarefree if and only if it is coprime with its derivative. If $\operatorname{char} F = 0$, then we see that f is squarefree if and only if $a = 1$. If however $\operatorname{char} F = p > 0$, then f is squarefree if and only if $a = 1$ and p does not divide b. Thus Theorem 1 completes the proof. □

Let $m = p_1^{a_1} \cdots p_k^{a_k}$ be a positive integer, where $p_1 < \cdots < p_k$ are primes. Suppose that we want to describe all finite ring constructions

$$R = \mathbb{Z}_m[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$$

whose radicals are principal ideals. Since $\mathbb{Z}_m$ is isomorphic to the direct product $\prod_{i=1}^{k} \mathbb{Z}/p_i^{a_i}\mathbb{Z}$, and the radical of a finite direct product is a principal ideal if and only if the radicals of all direct components are principal, it easily follows that we need only to consider the case where $m = p^a$ for a prime p.

Let $m = p^a$. Any element of $\mathbb{Z}_m$ is uniquely represented by an element of the integer interval $[0, m-1] = \{0, 1, \ldots, m-1\} \subseteq \mathbb{Z}$. Denote by $\mathcal{B}[x]$ the set of all polynomials $f \in \mathbb{Z}_m[x]$ such that all coefficients of f are represented by elements of $\mathcal{B} = [0, p-1]$. Let $f \longmapsto \overline{f}$ denote the natural homomorphism of $\mathbb{Z}_m[x]$ onto $\mathbb{Z}_p[x]$ (i.e., reduction of coefficients modulo p).

Obviously, for any polynomial $g \in \mathbb{Z}_p[x]$ there exists a unique polynomial $g' \in \mathcal{B}[x]$ such that $\overline{g'} = g$. Hence, for any polynomial $f \in \mathbb{Z}_m[x]$ there exists a unique polynomial $f' \in \mathcal{B}[x]$ such that $\overline{f'} = \overline{f}$. Evidently, $\overline{f} = \overline{g}$ if and only if $f' = g'$.

Similarly, if $a > 1$, then there exists a unique polynomial $f'' \in \mathcal{B}[x]$ such that $f - f' - pf'' \in p^2\mathbb{Z}_m$. For $a = 1$, we put $f'' = 0$.

Using this terminology, for any $f \in \mathbb{Z}_m[x]$, with $\operatorname{sp}(f)$ being the squarefree part of f, we define unique polynomials $d, u = u_f \in \mathcal{B}[x]$ and $\widehat{f} \in \mathbb{Z}_p[x]$ by the following conditions, $d = \operatorname{sp}(f)'$, $u = u'$, $\overline{f} = \overline{d}\overline{u}$ and $\widehat{f} = \overline{f'' - (ud)''}$. It follows that $\overline{d} = \operatorname{sp}(\overline{f})$ and $f' - ud \in p\mathbb{Z}_m[x]$. Since $f' \in \mathcal{B}[x]$ then $(f')'' = 0$ for any f and we also get $\widehat{f} = \overline{f'' + (f' - ud)''}$.

Theorem 4 *Let $m = p^a$, where p is a prime and a is a positive integer. The radical of the ring*

$$R = \mathbb{Z}_m[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$$

is a principal ideal if and only if the following conditions are satisfied:

(i) the number of polynomials $f_1, \ldots, f_n$ which are not squarefree modulo p does not exceed one;

(ii) if $a > 1$ and $f = f_i$ is not squarefree modulo p, then $\widehat{f}$ is coprime with $\overline{u_f}$.

P r o o f of Theorem 4. If $a = 1$, then $\mathbb{Z}/p^a\mathbb{Z}$ is a field, and the assertion follows from Theorem 1. Further, we assume that $a \geq 2$.

The radical $\mathcal{N}(R)$ contains the ideal pR, because $(pR)^a = 0$. If all polynomials $\overline{f}_1(x_1), \ldots, \overline{f}_n(x_n)$ are squarefree over $\mathbb{Z}_p$, then

$$R/pR \cong \mathbb{Z}_p[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$$

is semisimple by Lemma 2, and so $\mathcal{N}(R) = pR$ is a principal ideal.

Suppose that exactly one polynomial, say $f = f_1$, is not squarefree. Let u, d be polynomials in $\mathbb{Z}_m[x]$ as defined above then it follows from Lemma 2 that

$$\mathcal{N}(R) = (d, p) = \{\mathcal{N}(\mathbb{Z}_m[x_1]/(f_1))\}[x_2, \ldots, x_n]/(f_2, \ldots, f_n).$$

Therefore $\mathcal{N}(R)$ is a principal ideal if and only if $\mathcal{N}(\mathbb{Z}_m[x_1]/(f_1))$ is principal. So we may assume that $n = 1$, $x = x_1$, and $R = \mathbb{Z}_m[x]/(f(x))$.

Suppose that $\widehat{f}$ is coprime with $\overline{u_f} = \overline{u}$. Denote by h a polynomial in $\mathbb{Z}_m[x]$ such that $h = h'$ and $\overline{h}$ is the product of all irreducible divisors of $\overline{f}$ which do not divide $\widehat{f}$. Put $g = d + ph \in \mathbb{Z}_m[x]$. We claim that the radical $\mathcal{N}(R)$ is equal to the ideal I generated in R by g.

It follows from Lemma 2 that $\mathcal{N}(R) = (p, d)$. hence $g \in \mathcal{N}(R)$ so $I \subseteq \mathcal{N}(R)$. Therefore it remains to show that $p, d \in (g) = I$.

The choice of h ensures that $\widehat{f} - \overline{hu}$ is not divisible by any irreducible factor of $\overline{f}$ which does not divide $\widehat{f}$. If we look at an irreducible factor of $\overline{f}$ which divides $\widehat{f}$, then it does not divide $\overline{h}$, and so it does not divide $\overline{hu}$, because $\overline{u}$ is coprime with $\widehat{f}$. Thus $\widehat{f} - \overline{hu}$ and $\overline{d}$ are coprime.

Hence there exist $A, B \in \mathbb{Z}_m[x]$ such that $A = A'$, $B = B'$ and $\overline{1} = \overline{A}(\widehat{f} - \overline{hu}) + \overline{B}\overline{d}$. Notice that $f' - ud = p[(f' - ud)''] + p^2 w$ for some $w \in \mathbb{Z}_m[x]$, because $(f' - ud)' = 0$. There exists a unique polynomial $f^* = (f^*)' \in \mathbb{Z}_m[x]$

satisfying $\overline{f^*} = \widehat{f}$. Since p^a is the characteristic of $\mathbb{Z}_m$ then $p^a w = 0$ for all $w \in \mathbb{Z}_m[x]$. We can lift the equation from $\mathbb{Z}_m[x]/p\mathbb{Z}_m[x] \cong \mathbb{Z}_p[x]$ to $\mathbb{Z}_m[x]$ and multiply by p^{a-1} to get the following.

$$\begin{aligned} p^{a-1} &= p^{a-1}[A(f^* - hu) + Bd] \\ &= p^{a-1}[A\{f'' + (f' - ud)'' - hu\} + Bd] \\ &= p^{a-2}[A\{pf'' + (f' - ud) - phu\} + pBd] \\ &= p^{a-2}[A(f' + pf'') - Au(d + ph) + pBd] \\ &= p^{a-2}[Af - (Au - pB)g]. \end{aligned}$$

Therefore $p^{a-1} \in (g, f) \subset \mathbb{Z}_m[x]$, and so $p^{a-1} \in I$.

Since p^{a-1} belongs to both I and $\mathcal{N}(\mathbb{Z}_{p^a})$, we can factor out the ideal generated by p^{a-1} in R and consider the ideal $I/p^{a-1}I$ in $R/p^{a-1}R$. Also clearly $\mathbb{Z}_{p^a}/p^{a-1}\mathbb{Z}_{p^a} \cong \mathbb{Z}_{p^{a-1}}$. We identify $f, g \in \mathbb{Z}_{p^a}[x]$ with their images in $f, g \in \mathbb{Z}_{p^{a-1}}[x]$. We can now lift the equation from $\mathbb{Z}_p[x]$ to $\mathbb{Z}_{p^{a-1}}[x]$ and multiply by p^{a-2} and repeat the argument above with $p^{a-1}w = 0$ for all $w \in \mathbb{Z}_{p^{a-1}}[x]$ to get $p^{a-2} \in (g, f) \subset \mathbb{Z}_{p^{a-1}}[x]$. Identifying $p^{a-2} \in \mathbb{Z}_{p^a}[x]$ with its image $p^{a-2} \in \mathbb{Z}_{p^{a-1}}[x]$ then $p^{a-2} \in I/p^{a-1}I$ so $p^{a-2} \in I$. Repeating this argument $a - 3$ times we get $p \in I$.

Next we prove that $d \in I$. Since $g, p \in I$ then $d = g - ph \in I$. Thus $I = \mathcal{N}(R)$. This means that $\mathcal{N}(R)$ is a principal ideal.

Conversely, suppose that the radical is a principal ideal generated by some polynomial $g \in \mathbb{Z}_m[x]$.

Since $(\overline{g}) = (\overline{d}) = \mathcal{N}(\mathbb{Z}_p[x]/(\overline{f}))$, we get $\overline{g} = \overline{t}\overline{d} + \overline{e}\overline{f}$ for some $t = t' \in \mathbb{Z}_m$ and $e(x) \in \mathbb{Z}_m[x]$. There exists an integer $s = s' \in \mathbb{Z}_m$ such that $ts \equiv 1 (\bmod p)$. Since $\overline{s(g - ef)} = \overline{std} = \overline{d}$ and $(\overline{g}) = (\overline{d})$ then g generates the same ideal as $s(g - ef)$ in $R = \mathbb{Z}_m[x]/(f)$, so we can replace g by $s(g - ef)$. To simplify the notation we assume that $\overline{g} = \overline{d}$, and so $g' = d$.

Given that $p \in \mathcal{N}(R)$, we get $p = Af + Bg$ for some $A, B \in \mathbb{Z}_m[x]$. Since $(Af + Bg)' = (A'f' + B'g')' = 0$, it follows that $\overline{A'f'} + \overline{B'g'} = 0$. Therefore $\overline{B'} = -\overline{A'}\overline{u}$ whence $B' = -A'u + pz$ for some $z = z' \in \mathbb{Z}_m[x]$.

Further, $p = (A' + pA'')(f' + pf'') + (B' + pB'')(g' + pg'') + p^2 w$, for some $w \in \mathbb{Z}_m[x]$. Notice that $f' = (ug')'$ because $\overline{f'} = \overline{f} = \overline{ug'}$. Since $u = u'$ and $g = g'$ then $ug' = (ug')' + p(ug')'' = f' + p(ug')''$. It follows that $f' - ug' = -p(ug')''$. Therefore we get

$$\begin{aligned} p^{a-1} &= p^{a-2}[(A' + pA'')(f' + pf'') + (-A'u + pz + pB'')(g' + pg'')] \\ &= p^{a-2}[A'(f' - ug' + pf'') - A'upg'' + pA''f' + pg'(z + B'')] \\ &= p^{a-1}[A'(-(ug')'' + f'') - uA'g'' + A''(ug')' + g'(z + B'')], \end{aligned}$$

Given that $p^a = 0$, then $p^{a-1}v = p^{a-1}w$ if and only if $\overline{v} = \overline{w}$ where $v, w \in \mathbb{Z}_m[x]$. Hence

$$\begin{aligned} \overline{1} &= \overline{A'}(\overline{-(ug')'' + f''}) - \overline{u}(\overline{A'g''}) + \overline{A''}(\overline{(ug')'}) + \overline{g'}(\overline{z + B''}) \\ &= \overline{A'}\widehat{f} - \overline{u}(\overline{A'g''}) + \overline{A''}\overline{u}\overline{g'} + \overline{g'}(\overline{z + B''}). \end{aligned}$$

Since all irreducible factors of $\overline{u}$ divide $\overline{g'} = \overline{d}$, they also divide the polynomial $-\overline{u}(\overline{A'g''}) + \overline{A''}\overline{u}\overline{g'} + \overline{g'}(\overline{z + B''})$, and we see that $\overline{u}$ must be coprime with $\widehat{f}$. This completes the proof. □

2. Hamming weights. Let $\mathbb{F}$ be a field, $a_1, \ldots, a_n$ nonnegative integers, $b_1, \ldots, b_n$ positive integers, and let

$$R = \mathbb{F}[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_n^{a_n}(1 - x_n^{b_n})).$$

Ideals of the form $(x_1^{a_1}(1-x_1^{b_1}), \ldots, x_n^{a_n}(1-x_n^{b_n}))$ are called periodic ideals (see [9] Definition 6.16 p.2817). Denote by I the radical $\mathcal{N}(R)$ of R. Lemma 2 tells us that I is generated by the squarefree parts of the polynomials $x_1^{a_1}(1 - x_1^{b_1})$. The *Hamming distance* or *minimum Hamming weight* $w_H(I)$ of I in the basis $B = \{x_1^{e_1} \cdots x_n^{e_n} | 0 \leq e_i < a_i + b_i \text{ for } 1 \leq i \leq n\}$ is the minimum number of nonzero coordinates in B of nonzero vectors in I. It is an important characteristic, and in particular determines the number of errors the code I can detect or correct (see [11]). Clearly, $w_H(\{0\}) = 0$. We shall give formulas for the Hamming weight of powers of I with respect to the basis B.

Let $w(r)$ be the Hamming weight of $r \in R$ and let $w(J)$ be the minimum Hamming weight of an ideal $J \subset R$ with respect to B.

Suppose that $\mathbb{F}$ has zero characteristic. We may assume that $a_1 \geq \ldots \geq a_k > 1$ and $a_{k+1}, \ldots, a_n \leq 1$. Then the radical I is generated by all polynomials $x_i(1 - x_i^{b_i})$, for $i = 1, \ldots, k$. It follows that I is also generated by all polynomials $g_i = x_i(1 - x_i^{b_i + a_i(b_i - 1)})$, for $i = 1, \ldots, k$. Since $g_i^{a_i} = 0$ and $g_i^j = x_i^j(1 - x_i^{b_i + a_i(b_i-1)})$ modulo $x_i^{a_i}(1 - x_i^{b_i})$, we see that the linear span of all powers g_i^j has Hamming weight 2, for $j = 1, \ldots, a_i - 1$. Therefore, the theorem in Section 2 of [13] gives us the following formula for the Hamming weight $w(I^h)$ of I^h:

$$w(I^h) = \begin{cases} 2^\ell & \text{if } a_1 + \cdots + a_{\ell-1} - \ell + 1 < h \leq a_1 + \cdots + a_\ell - \ell \\ 0 & \text{if } a_1 + \cdots + a_k - k \leq h. \end{cases}$$

Let $\mathbb{F}$ be a field of characteristic $p > 0$. First, we consider the case where $a_1 = \cdots = a_n = 0$.

For each $i = 1, \ldots, n$, we write $b_i = p^{c_i} d_i$ where p does not divide d_i. We may assume that $c = c_1 \geq c_2 \geq \ldots \geq c_n \geq 0$. Denote by $z \geq 0$ the number of elements $c_1, \ldots, c_n$ which are equal to 0 or, in other words, the number of elements $b_1, \ldots, b_n$ not divisible by p.

Then the radical I is generated by all elements $f_i = 1 - x^{d_i}$, for $i = 1, \ldots, n - z$.

Following Berman [3], for $a \geq 0$, denote by ℓ_a the number of exponents c_i such that $c_i > a$. In particular, $\ell_0 = n - z$ and $\ell_c = 0$. Put $m_a = \ell_a(p-1)p^a$.

The nilpotency index of I is $N = p^{m_0 + m_1 + \cdots + m_c}$. Suppose that $h < N$. Then there exists b such that $\sum_{a=b+1}^{c} m_a \leq h < \sum_{a=b}^{c} m_a$. We can find t such that $h = \sum_{a=b+1}^{c} m_a + t(p-1)p^b + s$ and $t(p-1)p^b \leq h - \sum_{a=b+1}^{c} m_a < (t+1)(p-1)p^b$. Then $w(I^h)$ is equal to the following number (see [3], [5] or [13])

$$w(h; c_1, \ldots, c_n) = \begin{cases} 0 & \text{if } h \geq p^{m_0 + m_1 + \cdots + m_c} \\ p^{\ell_{b+1} + \ell_{b+2} + \cdots + \ell_{b_c + t}}(1 + \lceil sp^{-b} \rceil) & \text{otherwise.} \end{cases}$$

Next, consider the case where $n = 1$. Put $a = a_1, b = b_1, c = c_1, d = d_1$. Then $R = I\!F[x]/(x^a(1-x^b))$ and $b = p^c d$. It is routine to verify that the radical of R is generated by $g = x(1 - x^{b + a(b-1)})$ and $f = x^a(1 - x^d)$. Since $x^{a-1}g = 0$, the linear span V of $g, xg, \ldots, x^{a-2}g$ annihilates f. Hence $I = V + (f)$. For any $v \in V$ and $y \in (f)$ it is clear that $w(v + y) \leq w(y)$. Exactly as in the case of characteristic zero, $w(V) = w(V^2) = \cdots = w(V)^{a-1} = 2$. For $h \geq a$, we get $I^h = (f)^h$. Thus we have the following formula

$$w(I^h) = \begin{cases} 2 & \text{if } h < a \\ w(h; c) & \text{otherwise.} \end{cases}$$

In the general case, the algebra R is a tensor product of ring constructions

$$R_i = I\!F[x_i]/(x^{a_i}(1 - x^{b_i})),$$

where $i = 1, \ldots, n$. The radical of R is generated by all $g_i = x_i(1 - x_i^{b_i + a_i(b_i - 1)})$ and $f_i = x_i^a(1 - x^{d_i})$. As we have seen, the weight of the radical I_i of every R_i is equal to the weight of an element of the form g_i^k or f_i^k for some positive integer k. It follows from the theorem in Section 2 of [13] that the weight of I^h is equal to the weight of some element of the form $q_1^{k_1}(x_1) \cdots q_n^{k_n}(x_n)$, where $q_i \in \{f_i, g_i\}$ and $k_1 + \cdots + k_n \geq n$. Therefore,

$$w(I^h) = \min \left\{ \prod w(I_i^{k_i}) \mid k_1 + \cdots + k_n \geq n; \text{ all } k_i \geq 0 \right\}.$$

Let $[1,n] = \{1,2,\ldots,n\}$. Denote by L the set of all i such that $a_i > p^{c_i}$. Let $S = [1,n]\backslash L$. For any $T \subseteq [1,n]$, put $a_T = \sum_{i\in T} a_i - |T|$. Combining the formula above with the formulas for the weights of I_i^h, we get the following

$$w(I^h) = \begin{cases} 2 & \text{if } h < a_1 + \cdots + a_{n-z} \\ \min\limits_{T\subseteq[1,n-z]} \{2^{|L|+|T|} w(h - a_L - a_T; S\backslash T)\} & \text{otherwise.} \end{cases}$$

References

[1] M. Atiyah and I. McDonald, Introduction to Commutative Algebra (Addison-Wesley, 1969).

[2] T. Becker and V. Weispfenning, Gröbner Bases. A Computational Approach to Commutative Algebra (Springer-Verlag, 1993).

[3] S.D. Berman, On the theory of group codes, Kibernetika **3** (1967), 31–39.

[4] P. Charpin, The extended Reed-Solomon codes considered as ideals of a modular algebra, Annals Discrete Math. **17** (1983), 171–176.

[5] P. Charpin, Une generalisation de la construction de Berman des codes de Reed et Muller p-aires, Comm. Algebra **16** (1988), 2231–2246.

[6] R. Gilmer, Multiplicative Ideal Theory (Marcel Dekker, New York, 1972).

[7] B. Glastad and G. Hopkins, Commutative semigroup rings which are principal ideal rings, Comment. Math. Univ. Carolinae 21 (1980), 371–377.

[8] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Information Theory 40 (1994), 301–319.

[9] V.L. Kurakin, A.S. Kuzmin, A.V. Mikhalev and A.A. Nechaev, *Linear recurring sequences over rings and modules*, Journal of Mathematical Sciences **76**(6) (1995) 2793–2915.

[10] P. Landrock and O. Manz, Classical codes as ideals in group algebras, Des. Codes Cryptogr. **2** (1992)(3), 273–285.

[11] R. Lidl and G. Pilz, Applied Abstract Algebra (Springer-Verlag, New York, 1984).

[12] A. Poli, Important algebraic calculations for n-variables polynomial codes, Discrete Math. **56** (1985), 255–263.

[13] H.N. Ward, Visible codes, Arch. Math. **54** (1990), 307–312.

Eingegangen am

Anschrift der Autoren:

Department of Mathematics
University of Tasmania
G.P.O. Box 252-37, Hobart
Tasmania 7001
Australia

e-mail: cazaran@hilbert.maths.utas.edu.au
e-mail: kelarev@hilbert.maths.utas.edu.au