Cyclic codes and minimal strong Gröbner bases over a principal ideal ring

G. H. Norton, Dept. Mathematics, Univ. of Queensland, Brisbane 4072
A. Salagean, Dept. Computer Science, Loughborough University
Loughborough LE11 3TU, UK

April 22, 2003

Abstract

We characterise minimal strong Gröbner bases of $R[x]$, where R is a commutative principal ideal ring and deduce a structure theorem for cyclic codes of arbitrary length over R. When R is an Artinian chain ring with residue field $\overline{R}$ and $\gcd(\mathrm{char}(\overline{R}), n) = 1$, we recover a theorem for cyclic codes of length n over R due to Calderbank and Sloane for $R = \mathbb{Z}/p^k\mathbb{Z}$.

1 Introduction

All rings in this paper are commutative. This work originates from two structure theorems: (i) for certain cyclic codes over $R = \mathbb{Z}/p^k\mathbb{Z}$, with p a prime and k an integer, $k \geq 2$, [5, Theorem 6] and (ii) for a minimal strong Gröbner basis (SGB) of an ideal of $D[x]$, D a principal ideal domain, [9]. Intuitively, the first resembled a 'minimal SGB'. Since we had already developed a theory of SGB's over an principal ideal *ring* in [15], it was natural to ask whether (i) and (ii) have a common provenance. We confirm this and generalise (i) to a cyclic code of arbitrary length over a principal ideal ring.

In more detail, a cyclic code of length n over a ring R is an ideal of $R[x]/\langle x^n - 1\rangle$. The structure theorem for cyclic codes over R of [5] requires that $\gcd(p, n) = 1$ and the proofs used non-trivial results from Commutative Algebra on the ideal structure of $R[x]/\langle x^n - 1\rangle$. A generalisation of [5, Theorem 6] to cyclic codes over an Artinian chain ring was given in [14]. We formalised the notion of a 'generating set in standard form', *loc. cit.*, Definition 4.1 and showed that a cyclic code has a *unique* generating set in standard form, [14, Theorem 4.4]. See also [19, Theorem 3.9].

In addition, we recover the generating set in standard form of a cyclic code over an Artinian chain ring R as a minimal SGB using [15]. This provides an alternative proof of [14, Theorem 4.4]. Moreover, a similar result holds for arbitrary n (see Theorem 4.2 and condition (iv)) and also for codes over a principal ideal ring (see Theorem 5.6).

We begin with some preliminaries on Artinian chain rings R (e.g. Galois rings) and then characterise the structure of minimal SGB's of $R[x]$; see Theorem 3.2. This result is similar to the principal ideal domain case of [9], recalled as Theorem 2.11; see also [18]. In Section 4, we show that if p is the chararacteristic of the residue field of R and $\gcd(p, n) = 1$, minimal SGB's coincide with generating sets in standard form for cyclic codes over R. In Section 5, we generalise the structure theorems for minimal SGB's mentioned above to a principal ideal ring. In the final section we discuss connections between minimal SGB's over R and the representation of a regular $f \in R[x]$ as $f = uf^*$ with f^* monic and u a unit in $R[x]$ of [10, Theorem XIII.6].

We have thus found a common background for the structure theorems of [1, 5, 9]. Some of the results of this paper appeared in [17]. We remark that Allan Steel has implemented an SGB algorithm in Version 2.8 of Magma [3] using Corollary 2.8, generalising Faugère's algorithm [7] to Galois rings.

Related work for the special case of a Galois ring A appears in [4], where an SGB is called a GB. Their approach depends on whether the elements of A are represented additively or multiplicatively. On the other hand our notion of reduction is independent of how the elements of A are represented and how the operations are performed in A, as needed for working over principal ideal rings in general.

More importantly, there is another strictly weaker notion of a (weak) GB over any ring, [1, Definition 4.1.13]. The key result [4, Theorem 2.5.10] depends on the characterisation of a (weak) GB (rather than an SGB) in terms of homogeneous syzygies of monomials in $R[x]$ given in [1, Theorem 4.2.3]. This means that [4, Theorem 2.5.10] only yields a (weak) GB and not necessarily an SGB as in [4, Definition 2.4.1]. It turns out a (weak) GB is an SGB over an Artinian chain ring, [15, Proposition 3.9], but this is point is not considered in [4].

Thus while one could potentially generalise parts of [4] to finite chain rings, we prefer to avoid circular arguments (i.e. appealing to [15, Proposition 3.9]), a 'pre-selected division algorithm' and homogeneous syzygies. For example, we need only specialise [15, Theorem 4.10] to the univariate case, as in Corollary 2.8 below. Finally, concerning the decoding application of [4], we note that a characterisation of the set of solutions of the key equation and a quadratic decoding algorithm for an alternant code over a finite chain ring appeared in [13]. We do not know if the decoding application in [4] runs in polynomial time.

2 Preliminaries

First some notation and known results on Artinian chain rings, SGB's and minimal SGB's.

2.1 Notation

Throughout this paper R will denote a principal ideal ring which is not a field. We write the ideal of R generated by $r_1, \ldots, r_m \in R$ as $\langle r_1, \ldots, r_m \rangle_R$. The ideal of $R[x]$ generated by $f_1, \ldots, f_m \in R[x]$ is written as $\langle f_1, \ldots, f_m \rangle$ and $\subset, \supset$ denotes strict inclusion. As usual, $f = \sum_{i=0}^{d} c_i x^i \in R[x]$ with $c_d \neq 0$ has degree $d = \deg(f)$; $\mathrm{lt}(f) = x^d$ is its leading term and $\mathrm{lc}(f) = c_d$ is its leading coefficient; we say that f is *monic* if $\mathrm{lc}(f) = 1$. The leading monomial of f is $\mathrm{lm}(f) = \mathrm{lc}(f)\mathrm{lt}(f)$ and we denote by $\mathrm{cont}\,(f)$ a *content* of f i.e. a gcd of all its coefficients, which is well-defined up to a unit by [15, Lemma 4.3(iii)].

2.2 Artinian chain rings

We will need the following structure theorem:

THEOREM 2.1 *([20, Theorem 33, Section 15, Ch. 4]) A principal ideal ring is isomorphic to a finite direct product of principal ideal domains and Artinian chain rings.*

Recall that a *chain ring* is a ring whose ideals are linearly ordered by inclusion, [6]. In this section, R will denote an Artinian chain ring. The main properties of R are:

PROPOSITION 2.2 *R is a local principal ideal ring with maximal ideal $\mathrm{J}(R)$; the elements of $\mathrm{J}(R)$ are nilpotent and the elements of $R \setminus \mathrm{J}(R)$ are units.*

Let γ be a fixed generator of $\mathrm{J}(R)$ and ν the nilpotency index of γ i.e. the smallest positive integer for which $\gamma^\nu = 0$. (i) The distinct proper ideals of R are $\langle \gamma^i \rangle_R$, $i = 1, \ldots, \nu - 1$. (ii) For any element $r \in R \setminus \{0\}$ there is a unique i and a unit u such that $r = u\gamma^i$, where $0 \leq i \leq \nu - 1$ and u is unique modulo $\gamma^{\nu-i}$. (iii) $\mathrm{Ann}(\gamma^i) = \langle \gamma^{\nu-i} \rangle_R$.

It is not hard to see that a local principal ideal ring is a chain ring. Thus Artinian chain rings are precisely the Artinian local principal ideal rings.

From now on, γ and ν will be as in Proposition 2.2. It follows that any $f \in R[x] \setminus \{0\}$ can be written as $\gamma^i g$ where $0 \leq i \leq \nu - 1$, $\deg(f) = \deg(g)$ and $\gamma \not| g$. The exponent i is uniquely determined and g is unique modulo $\gamma^{\nu-i}$.

For any $r \in R$, the canonical projection $\varphi_r : R \to R/\langle r \rangle_R$ induces a ring homomorphism $R[x] \to (R/\langle r \rangle_R)[x]$, which we also write as φ_r. Of course, φ_γ projects R onto its residue field $\overline{R} = R/\mathrm{J}(R)$, and in this case we write $\overline{f}$ for $\varphi_\gamma(f)$.

The next theorem is stated for finite local rings in [10], but the proofs only use the fact that R is local and that the maximal ideal is nilpotent and finitely generated; R itself need not be finite. Recall that a polynomial in $R[x]$ is called *regular* if it is neither a unit nor a zero-divisor.

THEOREM 2.3 ([10, THEOREMS XIII.2 AND XIII.6]) *Let* $f = \sum_{i=0}^{m} f_i x^i \in R[x] \setminus \{0\}$. *Then:* *(i)* f *is a zero-divisor iff* $\gamma | f_i$ *for* $i = 0, \ldots, m$; *(ii)* f *is a unit iff* f_0 *is a unit and* $\gamma | f_i$ *for* $i = 1, \ldots, m$; *(iii) If* f *is regular then there are* $f^*, u \in R[x]$ *such that* $f = uf^*$, u *is a unit and* f^* *is monic.*

The polynomials f^* and u in Theorem 2.3(iii) are constructed by Hensel lifting. We generalise the construction in Theorem 2.3(iii) to any polynomial in $f \in R[x] \setminus \{0\}$ by defining $f^* = \gamma^i g^*$ where $\gamma^i \in \mathrm{cont}\,(f)$ and $f = \gamma^i g$. It follows that there is a unit $u \in R[x]$ such that $f = uf^*$. It is easy to show that f^* is unique in the sense that it satisfies the following property:

$$\text{if } f = vh, v \text{ a unit in } R[x] \text{ and } \mathrm{lc}(h) = \gamma^i \in \mathrm{cont}\,(f), \text{ then } h = f^*. \tag{1}$$

Also, the unit u is unique modulo $\gamma^{\nu - i}$.

The following consequence of Property (1) will be used later.

LEMMA 2.4 *Let* $f \in R[x] \setminus \{0\}$ *and* $\gamma^i \in \mathrm{cont}\,(f)$. *Then* $\deg(f^*) = \deg(\varphi_{\gamma^{i+1}}(f))$.

PROOF. Write $f = \gamma^i g$. By definition, $f^* = \gamma^i g^*$ and there is a unit $u \in R[x]$ such that $f = \gamma^i u g^*$. Applying the homomorphism $\varphi_{\gamma^{i+1}}$ we obtain $\varphi_{\gamma^{i+1}}(f) = \varphi_{\gamma^{i+1}}(\gamma^i u)\varphi_{\gamma^{i+1}}(g^*)$. By Theorem 2.3(ii), $\deg(\varphi_{\gamma^{i+1}}(u\gamma^i)) = 0$. Since g^* is monic, $\deg(\varphi_{\gamma^{i+1}}(g^*)) = \deg(g^*) = \deg(f^*)$. Hence $\deg(\varphi_{\gamma^{i+1}}(f)) = \deg(f^*)$. $\bowtie$

2.3 Strong Reduction and Strong Gröbner Bases

Let $f, g, h \in R[x]$. We write $f \twoheadrightarrow_G h$ if f *strongly reduces to* h *wrt.* G *in one step* and also say that f is *strongly reducible wrt.* G (see [1, p. 252] for the definition of strong reduction). The reflexive and transitive closure of $\twoheadrightarrow_G$ is denoted $\twoheadrightarrow_G^*$. When $f \twoheadrightarrow_G^* h$ we say that f *strongly reduces to* h *wrt.* G. If h is not strongly reducible wrt. G then h is a *remainder* of f wrt. G (by strong reduction). The set of such remainders is $\mathrm{SRem}(f, G)$. We adopt the conventions $0 \twoheadrightarrow_G^* 0$ and $\mathrm{SRem}(0, G) = \{0\}$ for any set G. Note that for any polynomial f there is at least one remainder of f wrt. G (by strong reduction) and if $f \twoheadrightarrow_G^* 0$ then $f \in \langle G \rangle$. As in the case of a field, we have:

THEOREM 2.5 *Let* I *be a non-zero ideal of* $R[x]$ *and* G *a finite subset of* $I \setminus \{0\}$. *The following assertions are equivalent: (i) any* $f \in I$ *is strongly reducible wrt.* G; *(ii)* $f \in I$ *if and only if* $f \twoheadrightarrow_G^* 0$; *(iii)* $f \in I$ *if and only if* $\mathrm{SRem}(f, G) = \{0\}$.

Let I be a non-zero ideal of $R[x]$ and G a finite subset of $I \setminus \{0\}$. Then G is a *strong Gröbner basis (SGB)* for I if it satisfies any of the conditions of Theorem 2.5. If G is an SGB for an ideal I, then $I = \langle G \rangle$. When we say 'G is an SGB', we will mean G is an SGB for $\langle G \rangle$. We will also appeal to:

Proposition 2.6 *([15, Corollary 3.12, Proposition 4.2]) Let $f \in R[x]$. Then $\{f\}$ is an SGB if and only if $f = rg$ for some $r \in R \setminus \{0\}$ and $g \in R[x]$ such that $\mathrm{lc}(g)$ is not a zero-divisor.*

In [15], we characterised SGB's for ideals of $R[x_1, \ldots, x_n]$ in terms of S- and G-polynomials (see [2, Definition 10.9]) of pairs of polynomials and 'A-polynomials': an A-polynomial of f is any polynomial af where $\mathrm{Ann}(\mathrm{lc}(f)) = \langle a \rangle_R$ [15, Definition 4.9]. Sets of S-, G- and A-polynomials are denoted $\mathrm{Spol}(f_1, f_2)$, $\mathrm{Gpol}(f_1, f_2)$ and $\mathrm{Apol}(f)$ respectively.

We now restate [15, Corollaries 5.12 and 5.13]) for univariate polynomials:

Corollary 2.7 *A finite subset G of $R[x]\setminus\{0\}$ is an SGB if and only if (A) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$, there is an $h \in \mathrm{Spol}(g_1, g_2)$ such that $h \twoheadrightarrow^*_G 0$; (B) for any $g \in G$, there is an $h \in \mathrm{Apol}(g)$ such that $h \twoheadrightarrow^*_G 0$; (C) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$ there is an $h \in \mathrm{Gpol}(g_1, g_2)$ which is strongly reducible wrt. to G.*

Algorithm SGB-PIR of [15] constructs an SGB from a finite set of generators using Corollary 2.7.

Corollary 2.8 *(Cf. [4, Theorem 2.5.10]) Let R be an Artinian chain ring. A finite subset G of $R[x] \setminus \{0\}$ is an SGB if and only if (A) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$, there is an $h \in \mathrm{Spol}(g_1, g_2)$ such that $h \twoheadrightarrow^*_G 0$ and (B) for any $g \in G$, there is an $h \in \mathrm{Apol}(g)$ such that $h \twoheadrightarrow^*_G 0$.*

2.4 Minimal SGB's

If G is an SGB, then G is *minimal* if no proper subset of G is an SGB for $\langle G \rangle$. One can easily see that an SGB G is minimal if for all distinct $f, g \in G$ we have $\mathrm{lm}(f) \not| \mathrm{lm}(g)$. Other properties of minimal SGB are described in [15, Section 7]. We recall some of these results for $R[x]$:

Corollary 2.9 *Let $G = \{g_0, \ldots, g_s\} \subset R[x]$ be an SGB. Then G is minimal if and only if for $i = 0, \ldots, s-1$ (i) $\langle \mathrm{lc}(g_i) \rangle_R \supset \langle \mathrm{lc}(g_{i+1}) \rangle_R$ and (ii) $\deg(g_i) > \deg(g_{i+1})$.*

Theorem 2.10 *Let $F = \{f_1, \ldots, f_k\}$ and $G = \{g_1, \ldots, g_l\}$ be minimal SGB's for an ideal I of $R[x]$. Then $k = l$ and there are units $u_i \in R$ such that after a suitable renumbering $\mathrm{lm}(f_i) = u_i \mathrm{lm}(g_i)$ for $i = 1, \ldots, k$.*

When R is a principal ideal domain, more is known about the structure of a minimal SGB. We recall a theorem based on [9]; see also [18]. Our formulation is close to the one in [1, Theorem 4.5.13 and Exercise 4.5.12].

Theorem 2.11 *Let D be a principal ideal domain which is not a field and let $G \subset D[x] \setminus \{0\}$. Then G is a minimal SGB if and only if $G = \{d_0 g_0, \ldots, d_s g_s\}$ for some $d_i \in D$, $g_i \in D[x]$ such that for $0 \leq i \leq s-1$, (i) $\langle d_i \rangle_R \supset \langle d_{i+1} \rangle_R$; (ii) $\mathrm{lc}(g_i) = \mathrm{lc}(g_{i+1})$; (iii) $\deg(g_i) > \deg(g_{i+1})$ and (iv) $d_{i+1} g_i \in \langle d_{i+1} g_{i+1}, \ldots, d_s g_s \rangle$. Moreover, $d_0 g_s = \gcd(d_0 g_0, \ldots, d_s g_s)$.*

3 Minimal SGB's over an Artinian chain ring

Throughout this section, R is an Artinian chain ring. The following result shows that all polynomials in a minimal SGB are of the form vf^*, v a unit in R.

PROPOSITION 3.1 *(i) Let $f \in R[x] \setminus \{0\}$. Any minimal SGB of $\langle f \rangle$ is equal to $\{vf^*\}$ for some unit $v \in R$. (ii) If G is a minimal SGB, then any $f \in G$ is equal to vf^* for some unit $v \in R$.*

PROOF. (i) This follows easily from Property (1) and Proposition 2.6. For (ii), let $f = vf^*$ where $v \in R[x]$ is a unit of minimal degree. It is enough to show that $\deg(f) = \deg(f^*)$. We know that $\deg(f) \geq \deg(f^*)$. Since $f^* = v^{-1}f \in \langle G \rangle$, $\mathrm{lm}(g)|\mathrm{lm}(f^*)$ for some $g \in G$. Hence if $\deg(f) > \deg(f^*)$, $\deg(f) > \deg(g)$ and $f \neq g$. This contradicts the minimality of G since $\mathrm{lm}(g)|\mathrm{lm}(f^*)|\mathrm{lm}(f)$. Hence $\deg(f) = \deg(f^*)$ and $v \in R$. $\bowtie$

Thus any principal ideal of $R[x]$ admits an SGB consisting of a single element. This is no longer the case if R is no longer an Artinian chain ring or the polynomials are no longer univariate; see [15, Examples 6.6, 6.12]. Corollary 2.9 can be improved, giving an analogue of Theorem 2.11:

THEOREM 3.2 *Let $G \subset R[x] \setminus \{0\}$. Then G is a minimal SGB if and only if $G = \{r_0g_0, \ldots, r_sg_s\}$ for some $s \leq \nu - 1$ where (i) $r_i = \gamma^{j_i}$ for $0 \leq j_0 < \cdots < j_s \leq \nu - 1$; (ii) $\mathrm{lc}(g_i)$ is a unit in R for $i = 0, \ldots, s$; (iii) $\deg(g_i) > \deg(g_{i+1})$ for $i = 0, \ldots, s-1$ and (iv) $r_{i+1}g_i \in \langle r_{i+1}g_{i+1}, \ldots, r_sg_s \rangle$ for $i = 0, \ldots, s-1$.*

PROOF. Let $G = \{f_1, \ldots, f_s\}$ be a minimal SGB. By Corollary 2.9 we may assume $\deg(f_i) > \deg(f_{i+1})$ for $i = 0, \ldots, s-1$. Define j_i by $\gamma^{j_i} \in \mathrm{cont}\,(f_i)$ for $i = 0, \ldots, s$ and write $f_i = \gamma^{j_i}h_i$ with $h_i \in R[x]$. By Proposition 3.1(ii), there are units $v_i \in R$ such that $f_i = v_if_i^* = v_i\gamma^{j_i}h_i^*$. If we now put $r_i = \gamma^{j_i}$ and $g_i = v_ih_i^*$ for $i = 0, \ldots, s$, then (i)-(iii) are easily checked. To prove (iv), let $h = r_{i+1}g_i - r_{i+1}g_{i+1}x^{\deg(g_i)-\deg(g_{i+1})} \in \langle G \rangle$. Since $h \twoheadrightarrow^*_G 0$ and $\deg(h) < \deg(g_i)$, only $r_{i+1}g_{i+1}, \ldots, r_sg_s$ can be used in the strong reduction, so $h \in \langle r_{i+1}g_{i+1}, \ldots, r_sg_s \rangle$. Hence $r_{i+1}g_i \in \langle r_{i+1}g_{i+1}, \ldots, r_sg_s \rangle$.

Conversely, assume that G is as in the theorem and $0 \leq i \leq s$. We will prove by induction on i that $G_i = \{r_ig_i, \ldots, r_sg_s\}$ is an SGB. The case $i = s$ follows from Proposition 2.6. Assume that $i < s$ and G_{i+1} is an SGB. Firstly, $\mathrm{Apol}(r_ig_i) = \{0\}$ since $\mathrm{lc}(g_i)$ is a unit. Now let $i \leq j < k \leq s$ and consider $h = r_kg_j - r_kg_kx^{\deg(g_j)-\deg(g_k)} \in \mathrm{Spol}(r_jg_j, r_kg_k)$. We first show that $h \in \langle G_{i+1} \rangle$, which is clear if $i < j$. If $j = i$ then $r_{j+1}g_j \in \langle G_{i+1} \rangle$ by (iv) and $r_{j+1}|r_k$, so $r_kg_j \in \langle G_{i+1} \rangle$ i.e. $h \in \langle G_{i+1} \rangle$. By the inductive hypothesis $h \twoheadrightarrow^*_{G_{i+1}} 0$ and therefore $h \twoheadrightarrow^*_{G_i} 0$. By Corollary 2.8, G_i is an SGB as required. Thus $G = G_0$ is an SGB, and it is minimal by Corollary 2.9. $\bowtie$

Condition (iv) of Theorem 3.2 implies that $\overline{g}_s|\overline{g}_{s-1}|\cdots|\overline{g}_0$. It might be expected that $r_0g_s|r_ig_i$ for $i = 0, \ldots, s$ as in Theorem 2.11. However, this is in general false:

EXAMPLE 3.3 *Let $R = \mathbb{Z}/8\mathbb{Z}$ and $G = \{x^4 - 1, 2(x^2+1), 4(x-1)\} \subset R[x]$. Putting $r_0 = 1$, $g_0 = x^4 - 1$, $r_1 = 2$, $g_1 = x^2 - 3$ and $r_2 = 4$, $g_2 = x - 1$, one easily sees that G is a minimal SGB by Theorem 3.2 and that $r_1 g_1$ is not divisible by $r_0 g_2$.* Moreover, no other minimal SGB $\{g'_0, 2g'_1, 4g'_2\}$ *(by Theorem 2.10)* for $\langle G\rangle$ has this property. *Using Theorems 2.10 and 3.2 and the fact that $2^i g'_i \twoheadrightarrow^*_G 0$ we see that, up to multiplication by units of R we can only have $2g'_1 = 2g_1$ or $2g'_1 = 2g_1 + 4g_2 = 2x^2 + 4x + 6$ and that $4g'_2 = 4g_2$ so $g'_2 = g_2 + 2a = x + 2a - 1$ for some $a \in R$. Evaluating $2g'_1$ at $x = 1, 3, 5, 7$ shows that $2g'_1$ is not divisible by g'_2.*

It is clear that if G satisfies Theorem 3.2(i),(ii),(iii) and (iv)' $g_s|\cdots|g_0$ then G is a minimal SGB. Example 3.3 also shows that the converse is not true in general. It is however true under certain circumstances:

THEOREM 3.4 *Let I be an ideal of $R[x]$. If there is a monic $f \in I$ with $\overline{f}$ square-free, then I has a minimal SGB $G' = \{r_0 g'_0, \ldots, g'_s\}$ which satisfies Theorem 3.2(i)-(iii), (iv)' above, $j_0 = 0$ and $g'_0|f$.*

PROOF. Let G be a minimal SGB for I as in Theorem 3.2. As f is monic and $f \twoheadrightarrow^*_G 0$, $j_0 = 0$. By (iv), $\overline{g_{i+1}}|\overline{g_i}$ for $i = 0, \ldots, s-1$. Also $\overline{g_0}|\overline{f}$ because $\overline{f} \in \overline{I} = \langle\overline{g_0}\rangle$. Putting $h_{-1} = \overline{f}/\overline{g}_0$, $h_i = \overline{g}_i/\overline{g}_{i+1}$ for $i = 0, \ldots, s-1$ and $h_s = \overline{g}_s$, we have $\overline{f} = h_{-1}h_0\cdots h_s$. Since $\overline{f}$ is square-free, the factors h_i are pairwise coprime and Hensel lifting yields $f = h'_{-1}h'_0\cdots h'_s$ with the h'_i monic, pairwise coprime and $\overline{h'}_i = h_i$ for $-1 \le i \le s$. Put $g'_i = h'_i \cdots h'_s$ for $0 \le i \le s$. It is easy to check that $g'_0|f$ and that G' satisfies (i)-(iv)'. Thus G' is a minimal SGB.

It remains to show that $\langle G'\rangle = I$. To show that $r_i g'_i \in I$ for $i = 0, \ldots, s$ we will use a technique similar to that of [5, Corollary of Theorem 6]. Since $\overline{g}_i = \overline{g'_i}$, $g'_i = g_i + \gamma l_i$ for some $l_i \in R[x]$. It suffices to show that $r_i\gamma l_i \in I$. We know that $g'_i|g'_0|f$, so $f = v_i g'_i$ for some $v_i \in R[x]$. Since $\overline{f} = \overline{v_i}\overline{g'_i} = \overline{v_i}\overline{g_i}$ and $\overline{f}$ is square-free, $\overline{v_i}$ and $\overline{g_i}$ are coprime. By [10, Theorem XIII.4] v_i and g_i are coprime in $R[x]$ i.e. $1 = av_i + bg_i$ for some $a, b \in R[x]$. Multiplying by $r_i\gamma l_i$ gives

$$r_i\gamma l_i = av_i(r_i\gamma l_i) + b(r_i\gamma l_i)g_i = av_i r_i(g'_i - g_i) + br_i\gamma l_i g_i = (ar_i)f + (b\gamma l_i - av_i)r_i g_i \in I$$

and so $\langle G'\rangle \subseteq I$. For the reverse inclusion, suppose that $h \in I \setminus \langle G'\rangle$ has minimal degree. Since G is an SGB for I, we have $\mathrm{lm}(r_j g_j)|\mathrm{lm}(h)$ for some j. But $\mathrm{lm}(r_j g'_j) = \mathrm{lm}(r_j g_j)$, so h is strongly reducible wrt. G', $h \twoheadrightarrow_{G'} h_1$ say. Then $h - h_1 \in \langle G'\rangle$, $h_1 \neq 0$ (otherwise $h \in I$) and $\deg(h_1) < \deg(h)$, for a contradiction. ⋈

REMARKS 3.5 *(i) The hypotheses of Theorem 3.4 can be relaxed to I having a minimal SGB $G = \{r_0 g_0, \ldots, r_s g_s\}$ of Theorem 3.2 with $r_0 = 1$ and $\overline{g}_i/\overline{g}_{i+1}$ pairwise coprime for $i = 0, \ldots, s-1$. (ii) The minimal SGB of Theorem 3.2 is similar to the 'canonical generating system (CGS)' of an ideal of $R[x]$, [11, Proposition 13], although GB's and cyclic codes were not mentioned in [11].*

A CGS has been generalised to an ideal I of $R[x_1,\dots,x_n]$ for which $R[x_1,\dots,x_n]/I$ is finitely generated in [12]. Some connections with Corollary 2.8 are discussed in [12, Section 5].

4 Cyclic codes over a finite chain ring

We now consider cyclic codes of arbitrary length n over an Artinian chain ring R. As usual, such codes correspond to ideals of $R[x]/\langle x^n-1\rangle$. Let $q: R[x]\to R[x]/\langle x^n-1\rangle$ be the quotient map. The following result is a straightforward generalisation of the corresponding result for fields (see [2, Theorem 9.19]).

PROPOSITION 4.1 *Let I be an ideal of $R[x]$ with $x^n-1\in I$ and let G be an SGB for I. Then for $f\in R[x]$, $q(f)\in q(I)$ if and only if $f\twoheadrightarrow^*_G 0$.*

Using Theorem 3.2 and Proposition 4.1 we obtain:

THEOREM 4.2 *Let $C\subset R[x]/\langle x^n-1\rangle$ be a non-zero cyclic code. There is an $s\le \nu-1$ and a $G=\{r_0g_0,\dots,r_sg_s\}\subset R[x]$ such that $q(G)$ generates C and (i) $r_i=\gamma^{j_i}$ for $i=0,\dots,s$ and $0\le j_0<\cdots<j_s\le\nu-1$; (ii) $\mathrm{lc}(g_i)$ is a unit for $i=0,\dots,s$; (iii) $n>\deg(g_0)>\cdots>\deg(g_s)$ and (iv) $r_{i+1}g_i\in\langle r_{i+1}g_{i+1},\dots,r_sg_s\rangle$ for $i=0,\dots,s-1$.*

Moreover $r_0(x^n-1)\twoheadrightarrow^*_G 0$ and if $\deg(f)<n$ then $q(f)\in C$ if and only if $f\twoheadrightarrow^*_G 0$.

Note that the last property of the preceding theorem gives an error-detection algorithm for C. Theorem 4.2 implies in particular that $\overline{g_s}|\cdots|\overline{g_0}|\overline{x^n-1}$. Since $\overline{x^n-1}$ is square-free if and only if $\gcd(\mathrm{char}(\overline{R}),n)=1$, Theorem 3.4 and Proposition 4.1 yield:

THEOREM 4.3 *If $\gcd(\mathrm{char}(\overline{R}),n)=1$, then Theorem 4.2 holds with property (iv) replaced by the stronger condition $g_s|\cdots|g_0|x^n-1$.*

The restriction $\gcd(\mathrm{char}(\overline{R}),n)=1$ is essential in Theorem 4.3 as Example 3.3 shows. The existence of a set of generators for a cyclic code as in Theorem 4.3 was proved in [5, Theorem 6] when $R=\mathbb{Z}/p^k\mathbb{Z}$ and $\gcd(p,n)=1$; see also [14, Theorem 3.17] and [8]. For negacyclic codes, constacyclic codes, or, more generally, codes which are ideals in $R[x]/\langle g\rangle$ for a given $g\in R[x]$, we can obtain analogues of Theorem 4.2 by simply replacing x^n-1 by g. If $\overline{g}$ is square-free, then we also obtain $g_s|\cdots|g_0|g$.

5 Minimal SGB's over a principal ideal ring

We generalise Theorems 2.11 and 3.2 to a principal ideal ring using some technical results collected in Subsection 5.1.

5.1 Preliminaries

Suppose that $A = A_1 \times \cdots \times A_m$ is a direct product of rings. The projections $\pi_i : A \to A_i$ induce maps $\pi_i : A[x] \to A_i[x]$. It is straightforward to check that the induced map $\pi : A[x] \to A_1[x] \times \cdots \times A_m[x]$ given by $\pi(f) = (\pi_1(f), \ldots, \pi_m(f))$ and the map $\kappa : A_1[x] \times \cdots \times A_m[x] \to A[x]$, which collects coefficients of like terms, are mutually inverse ring homomorphisms.

DEFINITION 5.1 *Let $G_i \subset A_i[x] \setminus \{0\}$ for $i = 1, 2$. Then $G_1 \sqcup G_2$, the* <u>*strong join*</u> *of G_1, G_2 is the subset $G_1 \times \{0\} \cup \{0\} \times G_2 \cup \{(t_1 g_1, t_2 g_2) \ : \ g_i \in G_i, t_i = \mathrm{lcm}(\mathrm{lt}(g_1), \mathrm{lt}(g_2))/\mathrm{lt}(g_i)\}$ of $A_1[x] \times A_2[x]$.*

It was shown in [16] that

THEOREM 5.2 *Let I be a non-zero ideal in $A[x]$ and $G_i \subseteq \pi_i(I) \setminus \{0\}$ for $i = 1, 2$. Then $\kappa(G_1 \sqcup G_2)$ is an SGB for I if and only if G_i is an SGB for $\pi_i(I)$ for $i = 1, 2$.*

We will use the following lemma:

LEMMA 5.3 *Any non-zero ideal of $R[x]$ has an SGB $\{r_0 g_0, \ldots, r_s g_s\}$ with $r_i \in R$, $\mathrm{lc}(g_i) = r$ for $i = 0, \ldots, s$ and $r \in R$ is not a zero-divisor.*

PROOF. If R is a principal ideal domain or an Artinian chain ring, the result follows by Theorem 2.11 and by Theorem 3.2, respectively. Suppose now that $R = R_1 \times R_2$ where R_1, R_2 are principal ideal rings such that the theorem holds in $R_1[x]$ and $R_2[x]$. We will show that the theorem holds for $R[x]$. Let I be an ideal in $R[x]$. By hypothesis, for $l = 1, 2$ there are $r^{(l)} \in R_l$ which are not zero-divisors, $s_l \geq 0$, $r_i^{(l)} \in R_l$, $g_i^{(l)} \in R_l[x]$ with $\mathrm{lc}(g_i^{(l)}) = r^{(l)}$ for $i = 0, \ldots, s_l$ such that $G^{(l)} = \{r_0^{(l)} g_0^{(l)}, \ldots, r_{s_l}^{(l)} g_{s_l}^{(l)}\}$ is an SGB for $\pi_l(I)$. Let $G = \kappa(G^{(1)} \sqcup G^{(2)})$. By Theorem 5.2, G is an SGB for I. Let $s = |G| - 1$ and denote by $f_0, \ldots, f_s$ the elements of G. Let $r = \kappa(r^{(1)}, r^{(2)})$. Since neither $r^{(1)}$ nor $r^{(2)}$ are zero-divisors, r is not a zero-divisor. For $k = 0, \ldots, s$ we will define $r_k \in R$ and $g_k \in R[x]$ such that $f_k = r_k g_k$ and $\mathrm{lc}(g_k) = r$. If $f_k = \kappa(r_i^{(1)} g_i^{(1)}, 0)$ for some $0 \leq i \leq s_1$, define $r_k = \kappa(r_i^{(1)}, 0)$ and $g_k = \kappa(g_i^{(1)}, r^{(2)} x^{\deg(g_i^{(1)})})$. If $f_k = \kappa(0, r_j^{(2)} g_j^{(2)})$ for some $0 \leq j \leq s_2$, define $r_k = \kappa(0, r_j^{(2)})$ and $g_k = \kappa(r^{(1)} x^{\deg(g_j^{(2)})}, g_j^{(2)})$. Finally, if

$$f_k = \kappa(r_i^{(1)} g_i^{(1)} x^{\max\{0, \deg(g_j^{(2)}) - \deg(g_i^{(1)})\}}, r_j^{(2)} g_j^{(2)} x^{\max\{0, \deg(g_i^{(1)}) - \deg(g_j^{(2)})\}})$$

for some $0 \leq i \leq s_1$ and $0 \leq j \leq s_2$, define $r_k = \kappa(r_i^{(1)}, r_j^{(2)})$ and

$$g_k = \kappa(g_i^{(1)} x^{\max\{0, \deg(g_j^{(2)}) - \deg(g_i^{(1)})\}}, g_j^{(2)} x^{\max\{0, \deg(g_i^{(1)}) - \deg(g_j^{(2)})\}}).$$

It is easy to verify now that $f_k = r_k g_k$ and $\mathrm{lc}(g_k) = r$ for $k = 1, \ldots, s$. The result now follows easily from Theorem 2.1. $\bowtie$

5.2 Characterisation of minimal SGB over a principal ideal ring

We now generalize Theorems 2.11 and 3.2 to a principal ideal ring:

THEOREM 5.4 *A finite set $G \subset R[x] \setminus \{0\}$ is a minimal SGB if and only if $G = \{r_0 g_0, \ldots, r_s g_s\}$ for some $r_i \in R$ and $g_i \in R[x]$ such that (i) $\langle r_i \rangle_R \supset \langle r_{i+1} \rangle_R$ for $i = 0, \ldots, s-1$; (ii) $\mathrm{lc}(g_i) = r$ for $i = 0, \ldots, s$ and r is not a zero-divisor; (iii) $\deg(g_i) > \deg(g_{i+1})$ for $i = 0, \ldots, s-1$ and (iv) $r_{i+1} g_i \in \langle r_{i+1} g_{i+1}, \ldots, r_s g_s \rangle$ for $i = 0, \ldots, s-1$.*

PROOF. Let $G = \{f_0, \ldots, f_s\}$ with $\deg(f_i) > \deg(f_{i+1})$ for $i = 0, \ldots, s-1$ be a minimal SGB for $I = \langle G \rangle$. By Lemma 5.3 there are $r \in R$, r not a zero-divisor, $s' \geq 0$, $r_i' \in R$, $g_i' \in R[x]$ with $\mathrm{lc}(g_i') = r$ for $i = 0, \ldots, s'$ such that $G' = \{r_0' g_0', \ldots, r_{s'}' g_{s'}'\}$ is an SGB for I. Without loss of generality, we may assume that G' is minimal. By Theorem 2.10, $s' = s$. By Corollary 2.9, we may also assume that $\deg(g_i') > \deg(g_{i+1}')$ and $\langle r_i' \mathrm{lc}(g_i') \rangle_R \supset \langle r_{i+1}' \mathrm{lc}(g_{i+1}') \rangle_R$ for $i = 0, \ldots, s-1$. Since $\mathrm{lc}(g_i') = r$ for all i, $\langle r_i' \rangle_R \supset \langle r_{i+1}' \rangle_R$. By Theorem 2.10 again, there are units $u_i \in R$ such that $\mathrm{lm}(f_i) = u_i \mathrm{lm}(r_i' g_i') = u_i r_i' \mathrm{lm}(g_i')$, for $i = 0, \ldots, s$. Now fix an i with $0 \leq i \leq s$. Since G' is an SGB for I and $f_i \in I$, we have $f_i \twoheadrightarrow^*_{G'} 0$. In this reduction only polynomials of degree at most $\deg(f_i) = \deg(g_i')$ can be used, so $f_i \in \langle r_i' g_i', \ldots, r_s' g_s' \rangle$. Since $r_i' | r_k'$ for all $i \leq k \leq s$, we have $r_i' | f_i$. So there is a $g_i \in R[x]$ such that $f_i = u_i r_i' g_i$. Since $\mathrm{lc}(f_i) = u_i r_i' \mathrm{lc}(g_i')$ we can choose $\mathrm{lc}(g_i)$ to be equal to $\mathrm{lc}(g_i') = r$. Putting $r_i = u_i r_i'$, we have $f_i = r_i g_i$ and conditions (i)-(iii) are verified. Condition (iv) can be checked as in the proof of Theorem 3.2.

Conversely, assume that G has the form $G = \{r_0 g_0, \ldots, r_s g_s\}$ with r_i, g_i having the properties specified in the statement of the theorem. We will prove that G is an SGB using Corollary 2.7. Conditions (A) and (B) follow by the same arguments as in the proof of Theorem 3.2. For condition (C), note that $r_i g_i \in \mathrm{Gpol}(r_i g_i, r_j g_j)$ is obviously strongly reducible wrt. G for any $0 \leq i < j \leq s$. Hence G is an SGB. The minimality of G follows from Corollary 2.9. ⋈

If G satisfies Theorem 5.4(i), (ii), (iii) and (iv)' $g_{i+1} | g_i$ for $i = 0, \ldots, s-1$ then G is a minimal SGB. However, condition (iv)' is not a necessary condition, as Example 3.3 shows. We saw that when R is an Artinian chain ring we have $\overline{g}_s | \overline{g}_{s-1} | \cdots | \overline{g}_0$. This weaker divisibility property is generalised below for principal ideal rings:

COROLLARY 5.5 *Let $G = \{r_0 g_0, \ldots, r_s g_s\}$ be a minimal SGB with r_i, g_i as in Theorem 5.4. For $i = 0, \ldots, s$, let $a_i \in R$ be such that $a_i r_i = r_{i+1}$ and $\langle a_i \rangle_R = (\langle r_{i+1} \rangle_R : r_i)$, with the convention $r_{s+1} = 0$. Then $\varphi_{a_j}(g_j) | \varphi_{a_j}(g_i)$ for all $0 \leq i < j \leq s$.*

PROOF. The existence of the a_i follows by [15, Proposition 5.1]. A simple induction on $j - i$ shows that $r_j g_i \in \langle r_j g_j, \ldots, r_s g_s \rangle$ for all $0 \leq i < j \leq s$. (The base of the induction follows from Theorem 5.4(iv)). Hence there are $h_j, \ldots, h_s \in R[x]$ such that $r_j g_i = r_j g_j h_j + r_{j+1} g_{j+1} h_{j+1} + \cdots +$

$r_s g_s h_s$. This can be rewritten as $r_j(g_i - g_j h_j) - r_{j+1} h = 0$ with $h = g_{j+1} h_{j+1} + a_{j+1} g_{j+2} h_{j+2} + \cdots + a_{j+1} \cdots a_{s-1} g_s h_s$ Hence $r_j(g_i - g_j h_j - a_j h) = 0$ i.e. each coefficient of $g_i - g_j h_j - a_j h$ is in $\mathrm{Ann}(r_j) = (\langle 0 \rangle_R : r_j) \subseteq (\langle r_{j+1} \rangle_R : r_j) = \langle a_j \rangle_R$. Hence $\varphi_{a_j}(g_i - g_j h_j - a_j h) = \varphi_{a_j}(g_i - g_j h_j) = 0$ i.e. $\varphi_{a_j}(g_j) | \varphi_{a_i}(g_i)$. $\bowtie$

Since Proposition 4.1 clearly applies to any ring, we deduce from Theorem 5.4:

THEOREM 5.6 *Let $C \subset R[x]/\langle x^n - 1 \rangle$ be a cyclic code over a principal ideal ring. There is a $G = \{r_0 g_0, \ldots, r_s g_s\}$ such that $q(G)$ generates C and $r_i \in R$, $g_i \in R[x]$ satisfy the properties (i)–(iv) in Theorem 5.4. Moreover, $\deg(g_0) < n$, $r_0(x^n - 1) \twoheadrightarrow^*_G 0$ and for any $f \in R[x]$ with $\deg(f) < n$ we have $q(f) \in C$ if and only if $f \twoheadrightarrow^*_G 0$.*

6 Some algorithmic consequences

Throughout this section R will be an Artinian chain ring. Let $f \in R[x] \setminus \{0\}$. We can compute f^* by Hensel lifting ([10, Theorem XIII.6]) or we can use Proposition 3.1(i) and compute a minimal SGB for $\langle f \rangle$ via Algorithm **SGB-FCR** of [15, Subsection 6.2]; see also [16, Appendix].

We now compare their worst-case complexities. If $n = \deg(f) \geq m = \deg(f^*)$ and $d = n - m + 1$, computing f^* by Hensel lifting has complexity $\mathcal{O}(\nu d m)$ since there are ν lifting steps, each requiring at most dm operations. Computing an SGB of $\{f\}$ requires $\mathcal{O}(\nu^2 d^3 n)$ since at most νd new polynomials (of degree at least m and at most n) will be added to the basis and computing the remainder of an S-polynomial or an A-polynomial will take at most dn operations. It is worth noting that by Lemma 2.4 we can stop the algorithm as soon as we obtain a polynomial of degree $\deg(\varphi_{\gamma^{i+1}}(f))$ in the basis, where $\gamma^i \in \mathrm{cont}\,(f)$.

Thus the worst-case complexity of Hensel lifting is somewhat lower than that of **SGB-FCR**($\{f\}$). In practice however, the complexity of Hensel lifting varies little with the particular input polynomial, whereas the complexity of computing an SGB varies significantly and the worst-case behaviour is rarely achieved. Examples suggest that Algorithm **SGB-FCR** may be more efficient in general for computing f^*.

Proposition 3.1(ii) yields a variant of Algorithm **SGB-FCR** for $R[x]$:

ALGORITHM 6.1 (SGB IN $R[x]$, R AN ARTINIAN CHAIN RING, USING THE *-CONSTRUCTION)
$G \leftarrow$ **SGB-FCR***(F)

Input: F a finite subset of $R[x]$, where R is a computable Artinian chain ring.
Output: G an SGB for $\langle F \rangle$.
Note: B is the set of pairs of polynomials in G whose S-polynomials still have to be computed.

begin $G \leftarrow \{g^*|g \in F\}$; $B \leftarrow \{\{f_1, f_2\}|f_1, f_2 \in G, f_1 \neq f_2\}$;

while $B \neq \emptyset$ **do**

select $\{f_1, f_2\}$ from B

$B \leftarrow B \setminus \{\{f_1, f_2\}\}$

compute $h \in \mathrm{Spol}(f_1, f_2)$

compute $g \in \mathrm{SRem}(h, G)$

if $g \neq 0$ **then** compute g^*; $B \leftarrow B \cup \{\{g^*, f\}|f \in G\}$; $G \leftarrow G \cup \{g^*\}$; **end if**

end while

return(G)

end

Note that g^* can be computed by Hensel lifting or via the original algorithm **SGB-FCR** $(\{g\})$, and that adding g^* rather than g to the basis is advantageous as $\deg(g^*) \leq \deg(g)$ and $\mathrm{lm}(g^*)|\mathrm{lm}(g)$.

Acknowledgements. Financial support from the U.K. Engineering and Physical Sciences Research Council (EPSRC) under Grant L07680 at the University of Bristol is gratefully acknowledged. The second author was partially supported by the EPSRC.

References

[1] W. Adams and P. Loustaunau. *An Introduction to Gröbner bases.* Graduate Studies in Mathematics 3. American Mathematical Society, 1994.

[2] T. Becker and V. Weispfenning. *Gröbner Bases, Graduate Texts in Mathematics 141.* Springer, 1993.

[3] W. Bosma, J. Cannon, and C.Playoust. The Magma algebra system I: The user language. *Journal of Symbolic Computation*, 24:235–265, 1997.

[4] E. Byrne and P. Fitzpatrick. Gröbner bases over Galois Rings with an application to decoding alternant codes. *Journal of Symbolic Computation*, 31:565–584, 2001.

[5] A. R. Calderbank and N. J. A. Sloane. Modular and p-adic codes. *Designs, Codes and Cryptography*, 6:21–35, 1995.

[6] R. Gilmer. *Multiplicative Ideal Theory.* Marcel Dekker, 1972.

[7] J.-C.Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *Journal of Pure and Applied Algebra*, 139:61–88, 1999.

[8] P. Kanwar and S. R. López-Permouth. Cyclic codes over the integers modulo $\mathbb{Z}_{p^m}$. *Finite Fields and Their Applications*, 3:334–352, 1997.

[9] D. Lazard. Ideal bases and primary decomposition: Case of two variables. *J. Symb. Comp.*, 1:261–270, 1985.

[10] B. R. McDonald. *Finite Rings with Identity.* Marcel Dekker, New York, 1974.

[11] A. A. Nechaev. Linear recurrence sequences over commutative rings. *Discrete Math. Appl.*, 2:659–683, 1992.

[12] A. A. Nechaev and D. A. Mikhailov. Canonical generating system of a monic polynomial ideal over a commutative artinian chain ring. *Discrete Math. Appl.*, 11:545–586, 2001.

[13] G. H. Norton and A. Salagean. On the key equation over a commutative ring. *Designs, Codes and Cryptography*, 20:125–141, 2000.

[14] G. H. Norton and A. Salagean. On the structure of linear and cyclic codes over finite chain rings. *Applicable algebra in engineering, communication and computing*, 10:489–506, 2000.

[15] G. H. Norton and A. Salagean. Strong Gröbner bases for polynomials over a principal ideal ring. *Bull. Australian Mathematical Society*, 64:505–528, 2001.

[16] G. H. Norton and A. Salagean. Gröbner bases and products of coefficient rings. *Bull. Australian Mathematical Society*, 65:147–154, 2002.

[17] G. H. Norton and A. Salagean. Strong Gröbner bases and cyclic codes over a finite-chain ring. *Workshop on Coding and Cryptography, Paris 2001. Electronic Notes in Discrete Mathematics*, 6, April, 2001. *http://www.elsevier.nl:80/inca/publications/store/5/0/5/6/0/9/.*

[18] G. Szekeres. A canonical basis for the ideals of a polynomial domain. *American Math. Monthly*, 59:379–386, 1952.

[19] Z.X. Wan. Cyclic codes over Galois Rings. *Algebra Colloq.*, 6:291–304, 1999.

[20] O. Zariski and P. Samuel. *Commutative Algebra*, volume 1. Springer, 1979.