The solution module (of n-dimensional sequences) of an ideal containing $(X_1^{M_1} - 1, \ldots, X_n^{M_n} - 1)$.

Graham H. Norton*

Centre for Communications Research
University of Bristol, England

July 9, 2001

Abstract

We study the solution module (of n-dimensional sequences over a domain R) of an ideal containing $(X_1^{M_1} - 1, \ldots, X_n^{M_n} - 1)$ and generalize the known (1-dimensional) result for the solution space of an ideal of $\mathbb{F}_q[X]$ containing $(X^M - 1)$. We show how to compute a groebner basis for the solution module, and apply this to compute the dual and check ideal of a 2-dimensional cyclic code (without using roots of unity or a semisimplicity hypothesis).

1 Introduction

This paper is a preliminary report on a constructive study of [1], [2], [3], [4], which were written before the advent of constructive ideal theory [5] and which require non-trivial Commutative Algebra (over a finite field). The first two papers are non-algorithmic in nature and are based on the zeroes of a code (and thus require a semisimplicity hypothesis); the work of Sakata is algorithmic but again requires non-trivial results from Commutative Algebra.

Our interest was to try to simplify the Commutative Algebra used in these papers by using constructive ideal theory (groebner bases). We also felt that this approach would be helped by clarifying the role of 2-D sequences. In particular, a goal was to compute the dual of a two-dimensional (2-D) cyclic code using the elements of Algebra and standard, established algorithms only, i.e. by what we may call *Elementary Algebra*, without using semisimplicity or noetherian hypotheses, nor the

*Research supported by U.K. Science and Engineering Research Council Grant GR/H15141. Current addresses: Dept. Mathematics, University of Queensland, Brisbane 4072, ghn@maths.uq.edu.au

variety associated with an ideal.

We begin the key 1-D result: let $\mathbb{F}$ be a finite field with q elements, $g \in \mathbb{F}[X]$ and let $\mathrm{Sol}(g)$ be the *solution space* of linear recurring sequences *(lrs)* annihilated by g. If $M \geq 1$, $g|(X^M - 1)$, $\gcd(q, M) = 1$ and g^* is the reciprocal of g, then $\mathrm{Sol}(g) \cong ((X^M - 1)/g^*)$. See e.g. [6, p79].

To state our main result for ideals of $R[X_1, \ldots, X_n]$, where $n \geq 1$ and R is any commutative domain, we need to give some additional notation. (See Sections 2 and 3 for precise definitions.)

Let $R[\mathbf{X}] = R[X_1, \ldots, X_n]$ and g^* denote the reciprocal of $g \in R[\mathbf{X}]$; $S^n(R)$ denotes the set of $\mathbb{N}^n$-indexed sequences of elements from R. Shifting defines an action of $R[\mathbf{X}]$ on $S^n(R)$, which we denote by $\circ$. If I is an ideal of $R[\mathbf{X}]$, let $\mathrm{Sol}(I)$ be the R-module $\mathrm{Sol}(I) = \{s \in S^n(R) : \forall f \in I, f \circ s = 0\}$.

We write P_M for the ideal $(X_1^{M_1} - 1, \ldots, X_n^{M_n} - 1)$, *on the understanding that* $M_i \geq 1$, for $1 \leq i \leq n$. For an ideal I of $R[\mathbf{X}]$, we write $\omega(I) \geq \mathbf{1}$ if some $P_M \subseteq I$. (For $n = 1$ and $I = (g), \omega(I) \geq 1$ if the order of g is at least one.)

We show in Section 3 that if $\omega(I) \geq \mathbf{1}$, there is a well-defined *(replicant) R-homomorphism* $\rho : \mathrm{Sol}(I) \to R[\mathbf{X}]/P_M$.

THEOREM 1. Let $n \geq 1, \omega(I) \geq \mathbf{1}$ and $P_M \subseteq I$. If $I = \sum_{j \in \mathbb{J}}(g_j)$, then the replicant homomorphism $\rho : \mathrm{Sol}(I) \to R[\mathbf{X}]/P_M$ induces

$$\rho : \mathrm{Sol}(I) \cong (P_M : \bigcup_{j \in \mathbb{J}} g_j^*)/P_M.$$

(Recall that for an *ideal* P and a *subset* S of $R[\mathbf{X}], (P : S) = \{f \in R[\mathbf{X}] : P \supseteq fS\}$ is the *ideal quotient* of P by S.) If $g|(X^M - 1)$, then $(X^M - 1 : g^*)$ is generated by $(X^M - 1)/g^*$, and we recover the 1-D result over R. Our proof does not use the roots of the generators of I and in particular, they do not have to be distinct.

In Section 4, we apply the ideal quotient algorithm of [7] (which uses groebner basis computations) to compute $\mathrm{Sol}(I)$ using standard, well established algorithms. Our algorithm has been implemented in MAPLE for all $n \geq 1$ and for all finite prime fields. Also, we can actually *write down* $\mathrm{Sol}(I)$ in certain cases which arise in practice (see Corollary 11).

We discuss 2-D cyclic codes in Section 5, computing the dual and check ideal of a 2-D cyclic code.

We take a "rootless" approach i.e. we do not use roots of unity and so do not need a semisimplicity hypothesis. Examples from [1] and [2] are recomputed. Finding a *reduced* groebner basis for the check ideal yields the "independent point set" of [4] and so enables us to design encoders for 2-D cyclic codes.

We conclude this Introduction with an overview of the notation. In general, we use Roman letters for elements, Greek letters for functions and short names for sets.

Notation	**Meaning**
$\mathbf{n}$	$\{1, 2, \ldots, n\}$.
π_i	Projection of $\mathbb{Z}^n$ onto the i^{th} component, $i \in \mathbf{n}$.
$\mathbf{X}^a$	Monomial $X_1^{a_1} \ldots X_n^{a_n}$, where $a_i \in \mathbb{Z}$.
$\delta_i f$	Degree of f in X_i, where $i \in \mathbf{n}$ and $f \in R[\mathbf{X}]$.
f^*	Reciprocal of $f \in R[\mathbf{X}]$.
P_M	$(X_1^{M_1} - 1, \ldots, X_n^{M_n} - 1)$, where $M_i \geq 1$ for $i \in \mathbf{n}$.
$S^n(R)$	n-dimensional sequences over R.
$\Gamma(s)$	Generating function of $s \in S^n(R)$, as element of $R[[\mathbf{X}]]$.
$f \circ s$	Polynomial f acting on s via shifting.
$\mathrm{Ann}(s)$	Characteristic ideal of s.
$\mathrm{Sol}(I)$	Solution module of an ideal I of $R[\mathbf{X}]$.
$[\,]$	Equivalence class of f in a quotient of $R[\mathbf{X}]$.

For $a, b \in A$, a commutative ring, (a, b) is the ideal generated by a and b and we write $a|b$ if b is a multiple of a. We equate sums and products over the empty set to 0 and 1 respectively.

2 Preliminaries

This paper is a sequel to [8] and we continue that notation for sequences, power series and polynomials.

We let $n \geq 1$, $\mathbf{n} = \{1, 2, ..., n\}$ and $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$; addition and negation in $\mathbb{Z}^n$ are defined componentwise. For $i \in \mathbf{n}, \pi_i : \mathbb{Z}^n \to \mathbb{Z}$ is the projection onto the i^{th} factor; we also write a_i for $\pi_i a$, where $a \in \mathbb{Z}^n$ and $i \in \mathbf{n}$. We let $\mathbf{0}, \mathbf{1}$ be the points in $\mathbb{Z}^n$ with all components 0, 1 respectively. (We use the notation $\mathbf{n}$ in the context of an index $i \in \mathbf{n}$, so that no confusion between $\mathbf{n}$ and $\mathbf{1} \in \mathbb{Z}^n$ arises.) $\mathbb{Z}^n$ is partially ordered by the relation $\leq$ on each component: $a \leq b$ iff $\pi_i a \leq \pi_i b$ *for all* $i \in \mathbf{n}$.

Let R be a commutative ring with 1 and let $R[\mathbf{X}] = R[X_1, \ldots, X_n]$ be the ring of polynomials in n commuting variables with coefficients from R; $R[[\mathbf{X}]]$ and $R((\mathbf{X}))$ have their usual meanings. For $g \in R((\mathbf{X})) \setminus \{0\}$, the subset $\mathrm{Supp}(g) = \{a \in \mathbb{Z}^n : g_a \neq 0\}$ of $\mathbb{Z}^n$ is called the *support* of g. We set $\mathrm{Supp}(0) = \emptyset$. Polynomials are those elements in $R[[\mathbf{X}]]$ of finite support.

The degree of $g \in R[X]$ is written δg (and $\delta 0 = -\infty$). For $f \in R[\mathbf{X}]$ and $i \in \mathbf{n}$, we let $\delta_i f$ be the i^{th} *partial degree* of f, that is, the degree of f regarded as a polynomial in X_i; δf is the n-vector with components $\delta_i f$. For $a \in \mathbb{Z}^n$, we abbreviate $X_1^{a_1} \ldots X_n^{a_n}$ to $\mathbf{X}^a$. If $f \in R[\mathbf{X}] \setminus \{0\}$, the reciprocal of f is $f^* = \mathbf{X}^{\delta f} f(X_1^{-1}, \ldots, X_n^{-1})$ and $0^* = 0$.

We write $f \in R[\mathbf{X}]$ as $f = f(\mathbf{X}) = \sum_{a \in \mathrm{Supp}(f)} f_a \mathbf{X}^a$.

It is clear that for $f \in R[\mathbf{X}] \setminus \{0\}, \delta_i f = \max\{a_i : a \in \mathrm{Supp}(f)\}$, so that for $a \in \mathrm{Supp}(f), \delta f - a$ is a well-defined point in $\mathbb{N}^n$.

If $f = \sum_{a \in \mathrm{Supp}(f)} f_a \mathbf{X}^a$, the reciprocal of f is $f^* = \sum_{a \in \mathrm{Supp}(f)} f_a \mathbf{X}^{\delta f - a}$. Clearly $\delta f^* \leq \delta f$; it is easy to verify that $f = \mathbf{X}^{\delta f - \delta f^*} f^{**}$ and that $(fg)^* = f^* g^*$.

An n-D sequence over R is simply a sequence of elements of R, indexed by $\mathbb{N}^n$: $S^n(R) = \{s : \mathbb{N}^n \to R\}$. If addition and scalar product are defined componentwise, $S^n(R)$ becomes a unitary R-module. There is an action of $R[\mathbf{X}]$ on $S^n(R)$ given by

$$\left(\sum_{a \in \mathrm{Supp}(f)} (f_a \mathbf{X}^a) \circ s \right)_b = \sum_{a \in \mathrm{Supp}(f)} f_a s_{a+b}$$

where $b \in \mathbb{N}^n$.

Thus $(\mathbf{X}^a \circ s)_b = s_{a+b}$. It is easy to check that $S^n(R)$ is an $R[\mathbf{X}]$-module and that $f \circ (g \circ s) = (fg) \circ s$, where fg denotes the product in $R[\mathbf{X}]$.

The annihilator ideal of s, $\mathrm{Ann}(s) = \{f \in R[\mathbf{X}] : f \circ s = 0\}$, is also called the *characteristic ideal* of s, and we say that s is an *(homogeneous) n-dimensional linear recurring sequence (n-D lrs)* if $\mathrm{Ann}(s) \neq \{0\}$.

Thus s is an n-D lrs if there is a non-zero $f \in R[\mathbf{X}]$ with $f \circ s = 0$. If $f = \sum_{a \in \mathrm{Supp}(f)} f_a \mathbf{X}^a$, then $f \circ s = 0$ is equivalent to

$$0 = (f \circ s)_b = \left(\sum_{a \in \mathrm{Supp}(f)} f_a \mathbf{X}^a \circ s \right)_b = \sum_{a \in \mathrm{Supp}(f)} f_a s_{a+b}$$

for all $b \geq \mathbf{0}$, and we recover the usual definition of an lrs. Finally, the generating function of $s \in S^n(R)$ is $\Gamma(s) = \sum_{a \geq \mathbf{0}} s_a \mathbf{X}^a \in R[[\mathbf{X}]]$.

3 The main result

We define the replicant homomorphism and state three lemmas which are used to prove the main result (Theorem 6).

DEFINITION 2. $\mathrm{Sol}(I)$, the *solution module* of an ideal I of $R[\mathbf{X}]$ is $\mathrm{Sol}(I) = \{s \in S^n(R) : I \subseteq \mathrm{Ann}(s)\}$.

The following lemma was stated for $S^n(\mathbb{F})$ in [9, Corollary 4.2], but is in fact valid for $S^n(R)$ (see [8, Corollary 2.11]):

LEMMA 3. Let $s \in S^n(R), p_i \in \mathrm{Ann}(s) \cap R[X_i]$ for $i \in \mathbf{n}$ and $p = \prod_{i=1}^n p_i$. Then $p^* \Gamma(s) \in R[\mathbf{X}]$ and $\delta_i p^* \Gamma(s) \leq \delta p_i - 1$ for $i \in \mathbf{n}$.

Thus if $\omega(I) \geq \mathbf{1}$ and $P_M \subseteq I$, there is a well-defined replicant homomorphism $\rho : \mathrm{Sol}(I) \to R[\mathbf{X}]/P_M$ given by $\rho(s) = [\prod_{i=1}^n (1 - X_i^{M_i}) \Gamma(s)]$.

Lemma 3 and the next lemma (which is a simple extension of [9, Lemma 2.2]) are used to show that the replicant map is 1-1.

LEMMA 4. (Reduction Lemma). Let R be a domain and $f = \sum_{i=1}^{n} p_i u_i$ for some $p_i \in R[X_i], u_i \in R[\mathbf{X}]$. There are $r \in R, v_i \in R[\mathbf{X}]$ such that $rf = \sum_{i=1}^{n} p_i v_i$ and for all $i \in \mathbf{n}$, $\delta p_i v_i \leq \delta f$.

The next result is used to show that ρ maps *onto* an ideal quotient. It was inspired by [10, Theorem 7.1, p 183], which applies to $S^1(\mathbb{F})$. (Note that in [10, loc. cit.], one-to-oneness is proved using a dimension argument over $\mathbb{F}$.)

We need several definitions before stating Lemma 5:

if $M \geq \mathbf{1}$ and $a \geq \mathbf{0}$, define $a \bmod M$ by $\pi_i(a \bmod M) = a_i \bmod M_i$ for all $i \in \mathbf{n}$ and if $\delta f \leq M - \mathbf{1}$, define $\sigma(f) \in S^n(R)$ by $\sigma(f)_a = f_{a \bmod M}$.

Clearly $\rho\sigma(f) = [f]$ if $\sigma(f) \in \mathrm{Sol}(I)$.

LEMMA 5. Let $M \geq \mathbf{1}$, $f,\ g \in R[\mathbf{X}], \delta f \leq M - \mathbf{1}$ and $M' \in \mathbb{N}^n$ be defined by $\pi_i(M') = (1 + \delta_i g/M_i)M_i$. Then

$$g^* f \equiv \sum_{\mathbf{0} \leq a \leq M - \mathbf{1}} (g \circ \sigma(f))_{a + M' - \delta g} \mathbf{X}^a (\bmod P_M)$$

The proof of Lemma 5 is a straightforward consequence of the definitions.

Recall that for an ideal P and a *subset* S of a commutative ring $A, (P : S) = \{a \in A : P \supseteq aS\}$. It is an ideal of A, called the *ideal quotient of P by S*, and it contains P. We write $(P : a)$ for $(P : \{a\})$. It is easy to check that $(P : \{a, b\}) = (P : a) \cap (P : b)$.

We can now state the main result:

THEOREM 6. Let $I = \sum_{j \in \mathbb{J}} (g_j) \subseteq R[\mathbf{X}],\ \omega(I) \geq \mathbf{1}$ and $P_M \subseteq I$. Then

$$\rho : \mathrm{Sol}(I) \cong \left(\bigcap_{j \in \mathbb{J}} (P_M : g_j^*) \right) / P_M.$$

4 Computing Ideal Quotients

We first show how we can write down certain ideal quotients that arise in practise and then give the main algorithm.

The following Lemma is proved for polynomial rings in [7, p256] but is in fact valid for any R.

LEMMA 7. Let $r \in R$ and let I be an ideal in R. If $I \cap (r) = (g_1, \ldots, g_k)$ then $(I : r) = (g_1/r, \ldots, g_k/r)$.

As a simple application,

PROPOSITION 8. If $g|p \in R$, then $(p : g) = (p/g)$.

LEMMA 9. Suppose that R is a factorial domain.

(a) Let $g_1(X_1)|f_1(\mathbf{X}) \in R[\mathbf{X}]$ and $f_i \in R[X_2, \ldots, X_n]$ for $2 \leq i \leq n$. Then

$$\left(\sum_{i=1}^{n}(f_i)\right) \cap (g_1) = (f_1) + \sum_{i=2}^{n}(g_1 f_i).$$

(b) If $g_i|p_i(X_i)$ then

$$(p_1, \ldots, p_n) \cap (\prod_{i=1}^{n} g_i) = \sum_{i=1}^{n}(p_i \prod_{i=1, j\neq i}^{n} g_j)$$

(c) If $g_i|p_i(X_i)$ then

$$\bigcap_{i=1}^{n}\left((g_i) + \sum_{j\neq i}(p_j)\right) = (\prod_{i=1}^{n} g_i) + (p_1, \ldots, p_n).$$

Combining Lemmas 7 and 9 parts (b), (c) now yields:

PROPOSITION 10 Let R be a factorial domain and let $g_i|p_i \in R[X_i]$ for $i \in \mathbf{n}$ and $P = (p_1, \ldots, p_n)$. Then

$$(P : \prod_{i=1}^{n} g_i) = \sum_{i=1}^{n}(p_i/g_i) \text{ and } (P : \sum_{i=1}^{n}(g_i)) = \left(\prod_{i=1}^{n} p_i/g_i\right) + P.$$

Combining the previous result with Theorem 6 (and identifying a polynomial and its equivalence class in $R[\mathbf{X}]/P_M$ for simplicity), we obtain

COROLLARY 11. Let R be a factorial domain, $g_i \in R[X_i]$, $M_i = \omega(g_i) \geq 1$. Then

$$\mathrm{Sol}(\prod_{i=1}^{n} g_i) \cong \sum_{i=1}^{n}(p_i/g_i^*)/P_M$$

$$\mathrm{Sol}(\sum_{i=1}^{n}(p_i/g_i^*) \cong (\prod_{i=1}^{n} g_i)/P_M$$

We remark that Corollary 11 yields reduced groebner bases for *any* term order. More generally, when R is a field $\mathbb{F}$, we can determine a lexicographic (reduced) groebner basis of any ideal quotient $((p_1, \ldots, p_n) : (g_1, \ldots, g_k))$, where $p_i \in \mathbb{F}[X_i]$, as follows:

ALGORITHM 12

Input: $n \geq 1,\ k \geq 1,\ g_j \in \mathbb{F}[\mathbf{X}]$ for $1 \leq j \leq k,\ P = (p_1, \ldots, p_n),\ p_i \in \mathbb{F}[X_i]$.

Output: A lexicographic (reduced) groebner basis for $(P : (g_1, \ldots, g_k))$.

(i) Using the $\mathbb{F}$-basis $\{\mathbf{X}^a : \mathbf{0} \leq a \leq \delta p - \mathbf{1}\}$ for $\mathbb{F}[\mathbf{X}]/P$, find an $\mathbb{F}$-basis $\{f_{1j}, f_{2j}, \ldots, f_{t_j j}\}$ for the (polynomial) solutions to $f_j g = 0$ in $\mathbb{F}[\mathbf{X}]/P,\ 1 \leq j \leq k$.

(ii) Compute a reduced groebner basis B_j for $\{f_{1j}, f_{2j}, \ldots, f_{t_j j}\} \cup P,\ 1 \leq k \leq k$.

(iii) Compute $\bigcap_{j=1}^{k} B_j$ as in [7, Section 4.3].

It follows that we can compute $\mathrm{Sol}(I)$ given a basis of any ideal I of $\mathbb{F}[\mathbf{X}]$ (which will be finitely generated by Hilbert's Basis Theorem). The following example is essentially [9, Example 3.5].

EXAMPLE 4.7. We compute $((p_1, p_2) : g)$, where $R = GF(2),\ p_i = X_i^4 + X_i^2 + 1, i = 1, 2$ and $g(X_1, X_2) = X_1^3 X_2^3 + X_1^3 X_2^2 + X_1^2 X_2^2 + X_1 X_2 + X_1 + 1$.

Step (i) yields the basis $\{X_1 X_2 + X_1 + 1,\ X_2 + X_1^3 + X_1 + 1,\ X_1^3 X_2^3 + X_1^3 X_2^2 + X_1^3 X_2 + X_1^3 + 1,$ $X_1^4 + X_1^2 + 1, X_1^2 X_2^3 + X_2^3 + X_1^2 X_2^2 + X_2^2 + X_1^2 X_2 + X_2 + X_1^2 + X_1 + 1,\ X_2^4 + X_1^3 X_2^3 + X_1 X_2^3 +$ $X_1^3 X_2^2 + X_1^3 X_2 + X_1 X_2^2 + X_1 X_2 + X_1^3 + X_1 + 1\}$

which has reduced groebner basis $\{X_2 + X_1^3 + X_1 + 1,\ X_1^4 + X_1^2 + 1\}$.

REMARKS 14

(i) It is easy to see that if $d_i = (p_i, g)$ and $d = d_1 \ldots d_n$, then $(P : g) = (\sum (p_i/d_i) : g/d)$, so we may assume without loss of generality in Algorithm 12 that for all $i,\ j,\ (p_i, g_j) = 1$.

(ii) Step (i) of Algorithm 12 is an application of [5, Method 6.7], which applies since $\{p_i : i \in \mathbf{n}\}$ is trivially a reduced groebner basis for the ideal it generates (with respect to any term order).

(iii) Step (ii) may be rendered more efficient using "k-elimination" term orderings. See [7, Chapter III] for details.

(iv) It is possible to generalize Algorithm 12 to more general domains. Firstly, as in [7], Step (i) can be done by computing a groebner basis of the $P \cap (g_j)$ and then applying Lemma 7. (This avoids solving linear systems over domains.) Secondly, more general groebner basis algorithms have been studied e.g. in Euclidean domains, [11] and in noetherian (M-L) rings, [12]. Thirdly, [7, Theorem 3.11] and the Elimination Theorem [7, Theorem 3.2] also hold in $R[\mathbf{X}]$ when R is noetherian (M-L) if we use [12, Theorems A, B]. As shown in [7, Section 3.3], this suffices to compute the intersection of two ideals and hence to compute a groebner basis for an ideal quotient in a noetherian (M-L) domain.

5 2-D cyclic codes

We define the dual and check ideal of a 2-D cyclic code and recompute some examples from [1], [2] and [3] using Algorithm 12.

Let $\mathbb{F}$ be a finite field, $M,\ N \geq 1$ and $P = (X^M - 1, Y^N - 1)$. Consider

$$c(X,Y) = \sum_{j=0}^{N-1} (\sum_{i=0}^{M-1} c_{ij} X^i) Y^j$$

$\in \mathbb{F}[X,Y]/P$, which also represents an $M \times N$ array of elements from $\mathbb{F}$. Multiplying $c(X,Y)$ by X (by Y) corresponds to a cyclic column (row) shift of c. Now a linear subspace of $\mathbb{F}[X,Y]/P$ is an ideal iff it is closed under multiplication by X and by Y. This motivates the following:

DEFINITION 15. ([13]) An $M \times N$ 2-D cyclic code over $\mathbb{F}$ is a proper ideal of $\mathbb{F}[X,Y]/P$.

EXAMPLE 16. (Product Codes) Let (f) and (g) be (M,k) and (N,l) cyclic codes respectively. The set of all $M \times N$ arrays in which the columns belong to (f) and the rows belong to (g) is closed under row and column shifts, and thus defines a 2-D cyclic code, called the *product code defined by* (f) *and* (g). It is well known and easy to prove that this product code is (fg). In particular, it is an (MN, kl) cyclic code.

The following example is from [1, p34].

EXAMPLE 17. Let $C_i,\ 1 \le i \le 5$ be the following ideals in $GF(2)[X,Y]/(X^3+1, Y^5+1)$:

$$C_1 = (X+1, Y+1),\ C_2 = (X^2+X+1, Y+1),\ C_3 = (X+1, Y^4+Y^3+Y^2+Y+1)$$

and

$$C_4\ = (X^2+X+1, Y^2+(X+1)Y+1),\quad C_5 = (X^2+X+1, Y^2+XY+1).$$

Observe that the last two are ideals since $(Y^2+(X+1)Y+1)(Y^2+XY+1) \equiv Y^4+Y^3+Y^2+Y+1 (\mathrm{mod} X^2+X+1)$. Also, none of these codes is a product code.

We define the dual of a 2-D cyclic code as in [1]:

DEFINITION 18. For $f, g \in \mathbb{F}[X,Y]/P$, define $f \perp g = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f_{ij} g_{ij} \in \mathbb{F}$. The dual of an $M \times N$ 2-D cyclic code C is

$$C^{\perp} = \{f \in \mathbb{F}[X,Y]/P : \forall g \in C, f \perp g = 0\}.$$

It is easy to see that $C^{\perp}$ is an ideal in $\mathbb{F}[X,Y]/P$. The next result gives two convenient polynomial characterizations of the dual code, and can be proved using [14, Theorem 1] and the fact that X and Y are invertible in $\mathbb{F}[X,Y]/P$.

PROPOSITION 19. Let C be an ideal of $\mathbb{F}[X,Y]/P$. Then in $\mathbb{F}[X,Y]/P$,

$$C^{\perp} = \{f : \forall g \in C, fg^* = 0\} = \{f : \forall g \in C, f^* g = 0\}.$$

COROLLARY 20. If $P \subseteq (g_1, \ldots, g_k)$, then

$$(g_1, \ldots, g_k)^{\perp} = \left(\bigcap_{j=1}^{k} (P : g_j^*) \right) / P.$$

COROLLARY 21. If $f|p$ and $g|q$, then

(a) $(fg)^{\perp} = (p/f^*, q/g^*)$ and

(b) $(f,g)^* = (pq/f^*g^*)$.

EXAMPLE 22. A codeword c of the $M \times N$ array code over $\mathbb{F}$ is an $M \times N$ array $[c_{ij}]$ satisfying $\sum_{i=1}^{M-1} c_{ij} = 0$ and $\sum_{j=0}^{N-1} c_{ij} = 0$. In other words, the column and row check polynomials are

$1 + X + \ldots + X^{M-1}$ and $1 + Y + \ldots + Y^{N-1}$. Thus the $M \times N$ array code is just the product code defined by $X - 1$ and $Y - 1$.

The duals of C_1, C_2 and C_3 in Example 5.3 are easily seen to be product codes by Corollary 5.7. However, for C_4 and C_5, we obtained

$$C_4^{\perp} = ((X+1)(Y+1)(Y^3+Y^2+X)),\ C_5^{\perp} = ((X+1)(Y+1)(Y^3+Y^2+X+1))$$

using Algorithm 12.

REMARK 23. The "dual ideals" calculated in [1,p34] are *not* the dual codes $C_i^{\perp}$, but the *check ideals* $C_i^{\vee}$: the check ideal of a 2-D cyclic code C is $C^{\vee} = \mathrm{Ann}_{\mathbb{F}[X,Y]}(C)$. It is easy to see that $C^{\vee} = (P : C)/P$. In particular, we can compute it using Algorithm 12. For example, to compute $C_4^{\vee}$, we find $((X^3+1, Y^5+1) : X^2+X+1)) \cap ((X^3+1, Y^5+1) : Y^2 + (X+1)Y + 1)$ is

$$(X+1, Y^5+1) \cap (X^3+1, Y^5+1, (X+1)(Y+1)(Y^2+XY+1))$$

which is

$$(X^3+1, Y^5+1, (X+1)(Y+1)(Y^2+XY+1))$$

so that $C_4^{\vee} = ((X+1)(Y+1)(Y^2+XY+1))$. Similarly, $C_5^{\vee} = ((X+1)(Y+1)(Y^2+(X+1)Y+1))$. Compare [1,p34].

Notice that $\dim_{\mathbb{F}} C_4^{\vee} = \dim_{\mathbb{F}} C_5^{\vee} = 5$ whereas $\dim_{\mathbb{F}} C_4^{\perp} = \dim_{\mathbb{F}} C_5^{\perp} = 2$. Thus in general, the dual and check ideal of a 2-D cyclic code are *not* equivalent subspaces, in contrast to 1-D cyclic codes.

EXAMPLE 24. Let $C_6 = ((X+1)(Y^2+X^2Y+1), (X^2+X+1)(Y+1))$ which is [2, Example 2a], and let C_7 be $(Y^4+Y^3+XY^2+(X^2+X+1)Y+X, (X+1)Y^3+(X^2+1)Y^2+(X^2+1)Y+X+1)$ which is [2, Example 3]. It is stated in [2] that $C_6^{\perp} = C_7$. However, we obtained $C_6^{\perp} = (Y^4+Y+X+1)$, not C_7 (as would be expected from the calculation on [2, p4,5]) and $C_7^{\perp} = (Y^3+Y^2+X+1)$.

The following example is partly due to A.Au:

EXAMPLE 25. Let $C_8 = ((X+1)(Y^2+XY+1), (X^2+X+1)(Y+1))$. Then $C_8^{\perp} = (XY^4+Y^3+Y^2+XY+X^2+X+1)$ and $C_8^{\perp\perp} = (Y^3+Y^2+X+1)$.

Thus $C_8 = C_7^{\perp}$, so $C_8^{\perp} = C_7$ and the first generator of C_6 above i.e. of [2, Example 2a] should be $(X+1)(Y^2+XY+1)$, not $(X+1)(Y^2+X^2Y+1)$. With this change, $C_6^{\perp} = C_7$.

EXAMPLE 26. Let $C_9 = (Y^2 + Y + X^2 + X)$ of [16, Example 6, p43]. We obtained $C_9^{\perp} = (Y^4 + Y^3 + Y^2 + Y + 1)(X^2 + X + 1)) = C_9^{\vee}$. In particular, $C_9^{\vee}$ and $C_9^{\perp}$ are equivalent, even though the generator of C_9 is not equal to its reciprocal.

6 Conclusion and Further Work

We have shown, using elementary techniques, that the solution module (of n-D sequences) of certain polynomial ideals is an explicit ideal quotient. This generalizes the known 1-D result to domains. We have also shown how to compute the solution module over fields using standard algorithms. As a consequence, we are able to compute the dual and check ideal (and hence encoders) of 2-D cyclic codes using standard algorithms.

It would be interesting to apply Section 5 to generalized array codes ([17],[18]) and to know, for a given a 2-D cyclic code C, when $C^{\perp}$ and $C^{\vee}$ are isomorphic $\mathbb{F}$-subspaces.

We also hope to apply the techniques of this paper to [19], [20].

ACKNOWLEDGEMENTS.The author would like to thank P. Fitzpatrick for helpful correspondence on 2-D codes, A. Au for implementing Algorithm 12 in MAPLE, as well as the U.K. Science and Engineering Council and the Centre for Communications Research for financial support.

References

[1] Ikai, T., Kosako, H. and Kojima, Y. Two dimensional cyclic codes. Electronics and Communications in Japan. Vol 57-A (1975), 27-35.

[2] Imai, H. A theory of two-dimensional codes. Inform. Control, Vol. 34 (1977) 1-21.

[3] Sakata, S. General theory of doubly periodic arrays over an arbitrary field and its applications. IEEE Trans. IT, Vol. IT-24 (1978), 719-730.

[4] Sakata, S. On determining the independent point set for doubly periodic arrays and encoding two-dimensional cyclic codes and their duals. IEEE Trans. IT, Vol IT-27 (1981) 556-565.

[5] Buchberger, B. Groebner bases: an algorithmic method in polynomial ideal theory. In "Multidimensional Systems Theory (N.K. Bose, ed.) Dordrecht: Reidel (1985), 184-232.

[6] van Lint, J.H. Introduction to Coding Theory. Springer Verlag, NewYork (1980).

[7] Cox, D., Little, J. and O'Shea, D. Ideals, Varieties and Algorithms. Springer Verlag. (1991).

[8] Norton, G.H. On n-dimensional sequences, I. Generating functions. Preprint, Dec 1991.

[9] Fitzpatrick, P. and Norton, G.H. Finding a basis for the characteristic ideal of an n-dimensional linear recurring sequence. IEEE Trans IT, Vol. IT-36 (1990), 1480-1487.

[10] Peterson, W. and Weldon, E.J. Error Correcting Codes (Second Edition) MIT Press, Cambridge Mass. 1972.

[11] Kandri-Rody, A. and Kapur, D. Computing a groebner basis of a polynomial ideal over a Euclidean domain. J. Symbolic Computation, Vol. 6 (1988), 37-57.

[12] Jacobsson, C. and Löfwall, C. Standard bases for general coefficient rings and a new constructive proof of Hilbert's basis theorem. J. Symbolic Computation, Vol. 12 (1991), 337-371.

[13] Berman, S.D. "Semisimple Cyclic and Abelian Codes II". Cybernetics, Vol. 3, No. 3, 17-23 (1967).

[14] McWilliams, J. Codes and Ideals in Group Algebras. In "Combinatorial Mathematics and its Applications". (Bose, R.C. and Dowling, T. Eds.). University of North Carolina Press, Chapel Hill (1969), 317 - 328.

[15] Blaum, M., Farrell, P.G. and van Tilborg, H.C.A. A class of burst error correcting array codes. IEEE Trans. IT, Vol. IT-32 (1986), 836 - 839.

[16] Imai, H. Multivariate polynomials in Coding Theory. Proceedings of AAECC-2, Springer Lecture Notes in Computer Science Vol. 228, 36-60.

[17] Blaum, M. and Roth, R.M. "New array codes for multiple phased burst correction." IEEE

Trans. Vol. IT- 39 (1993), 66 - 77.

[18] Honary, B., Markarian, G.S. and Farrell, P.G. "Generalised array codes and their trellis structure." Electronic Letters, Vol. 29 (1993), 541 - 542.

[19] Ikai, T., Kosako, H. and Kojima, Y. "Basic theory of two-dimensional cyclic codes. - periods of ideals and fundamental theorems." Electronics and Communications in Japan. Vol 59-A (1976), 31-38.

[20] Ikai, T., Kosako, H. and Kojima, Y. Basic theory of two-dimensional cyclic codes - structure of cyclic codes and their dual codes. Electronics and Communications in Japan. Vol 59-A (1976), 39-47.