Predictable degree property and row reducedness for a system over a semi simple ring

M. El Oued and P. Solé

***Abstract*— We study a linear discrete time dynamical system B on the finite ring $\mathbb{Z}_n$. A kernel representation theorem is derived. In the case of $n = p_1^{r_1} \dots p_m^{r_m}$ we introduce the notions of $(p_1, \dots, p_m)-$property for the predicted degree and of $(p_1, \dots, p_m)-$regularity.**

I. Introduction

In this work we consider a dynamical system $\Omega = (\mathbb{Z}+, \mathbb{Z}_n^q, B)$. Here B is the behavior of the system, i.e. a subset of $(\mathbb{Z}_n^q)^{\mathbb{Z}+}$. A kernel representation theorem is derived. In the case of $n = p_1^{r_1} \dots p_m^{r_m}$ we introduce the notions of $(p_1, \dots, p_m)-$property for the predicted degree and of $(p_1, \dots, p_m)-$regularity. These notions allow us to formulate a row reduceness theorem. Let σ denote the backward shift operator defined by $(\sigma w)(k) = w(k+1)$ for all w in B. We study the representation theory of σ on B and we give a kernel representation theorem. By annihilator of B we mean a polynomial vector $V(x) \in \mathbb{Z}_n^q[X]$ that satisfies for all $w \in B$ the relation $V(\sigma)w = 0$. We derive a necessary and sufficient condition for a polynomial, vector to be an annihilator of B. Thus, we generalize to arbitrary integers n the work of Kuijper et al. [1] which is the case of $n = p^r$.

The material is organized as follows. Section 2 establishes preliminary results on the submodules of $\mathbb{Z}_n^q$. Section 3 introduces the notion of reduced $p-$base for the submodules

II. Preliminary results on the submodules of $\mathbb{Z}_n^q$

We denote troughout by $n = p_1^{r_1} \dots p_m^{r_m}$ an arbitrary integer and by p one of the prime divisors of n.

Definition 1:

Let $v_1, \dots, v_k$ be a family of vectors of $\mathbb{Z}_n^q$. We call p-linear combination of $v_1, \dots, v_k$ any vector of the form

$$\sum_{i=1}^{k} a_i v_i$$

where $a_i \in \{0, 1, \dots, p-1\} \subset \mathbb{Z}_n$.

We denote by p-vect$(v_1, \dots, v_k)$ the set of all p-linear combinations of $v_1, \dots, v_k$.

Definition 2:

A family $v_1, \dots, v_k$ of $\mathbb{Z}_n^q$ is said to be p-generating if it satisfies

1) For all $1 \leq i \leq k-1$ the vector v_i can be written as a p-linear combination of the $v_{i+1}, \dots, v_k$.
2) $pv_k = 0$

Lemma 1:

If $v_1, \dots, v_k$ is $p-$generating then $p - vect(v_1, \dots, v_k) = vect(v_1, \dots, v_k)$.

In particular p-vect$(v_1, \dots, v_k)$ is a submodule of Z_n^q.

Definition 3:

A family $v_1, \dots, v_k$ of $\mathbb{Z}_n^q$ is said to be p-linearly independent if

$$a_1 v_1 + \dots + a_k v_k = 0$$

$\iff a_1 = \dots = a_k = 0$, for all $a_1, \dots a_k \in \{0, 1 \dots, p-1\}$.

In [1] a p-basis for a submodule M of $\mathbb{Z}_n^q$ is defined as a p-linearly independent p-generating family $(v_1, \dots, v_k)$ such that p-span$(v_1, \dots, v_k) = M$. and it was shown that every submodule of $\mathbb{Z}_{p^r}^q$ affords a p-basis. This is generalized in the following

Theorem 1:

If M is a submodule of $\mathbb{Z}_n^q$, then

$$M = \bigoplus_{i=1}^{m} M_i,$$

where for each M_i there exists a family $(v_1^i, \dots, v_{k_i}^i) \subset \mathbb{Z}_n$ that is p_i-generating, p_i-linearly independent and such that $M_i = p_i$-vect$(v_1^i, \dots, v_{k_i}^i)$.

Let $M = vect(v_1, \dots, v_k)$ a submodule of $\mathbb{Z}_n^q$ and write $M = \bigoplus_{i=1}^{m} M_i$. The family

$$(\frac{n}{p_i^{r_i}} v_1, \dots, \frac{n}{p_i} v_1, \dots, \frac{n}{p_i^{r_i}} v_k, \dots, \frac{n}{p_i} v_k)$$

is p_i-generating. Now we apply a Gaussian elimination algorithm gives in [2], we obtained a p_i-linearly independent p_i-generating family $(v_1^i, \dots, v_{k_i}^i)$ such that $M_i = p_i - vect(v_1^i, \dots, v_{k_i}^i)$.

III. $p-$reduced basis for the submodules of $\mathbb{Z}_n^q[X]$

In this section similar results are proved for modules over the polynomial ring $\mathbb{Z}_n^q[X]$.

Definition 4: Let $v_1(x), \dots, v_k(x)$ denote a family of $\mathbb{Z}_n^q[X]$ and let $a_i(x)$ be polynomials with coefficients in $\{0, \dots, p-1\} \subset \mathbb{Z}_n$. With this notation the vector

$$\sum_{i=1}^{k} a_i(x) v_i(x)$$

is call $p-$linear combination of the $v_1(x), \dots, v_k(x)$. The set of all such $p-$linear combination of the $v_1(x), \dots, v_k(x)$ is denoted by p-vect$(v_1(x), \dots, v_k(x))$.

Telecom ParisTech, CNRS/LTCI, Dept Comelec, 46 rue Barrault, 75 013 Paris sole@enst.fr

ISBN 978-963-311-370-7

Definition 5:
A family of vectors $(v_1(x),\ldots,v_k(x))$ of $\mathbb{Z}_n^q[X]$ is said to be $p-$generating if

1) For all $1 \leq i \leq k-1$, the vector $pv_i(x)$ is a $p-$linear combination of the $v_{i+1}(x),\ldots,v_k(x)$
2) $pv_k(x)$ is zero

Lemma 2:
If $(v_1(x),\ldots,v_k(x)) \subset \mathbb{Z}_n^q[X]$ is a $p-$generating family then

$$p - vect(v_1(x),\ldots,v_k(x)) = vect(v_1(x),\ldots,v_k(x)).$$

In particular, p-vect$(v_1(x),\ldots,v_k(x))$ is a submodule of $\mathbb{Z}_n^q[X]$.

Definition 6:
A family $(v_1(x),\ldots,v_k(x))$ de $\mathbb{Z}_n^q[X]$ is said to be $p-$linearly independent if there is no non trivial $p-$linear combination of the $(v_1(x),\ldots,v_k(x))$ that vanishes.

Lemma 3:
If $(v_1(x),\ldots,v_k(x)) \subset \mathbb{Z}_n^q[X]$ is a $p-$generating family that is also $p-$linearly independent then every vector of p-vect$(v_1(x),\ldots,v_k(x))$ can be written uniquely as a $p-$linear combination of $(v_1(x),\ldots,v_k(x))$.

Definition 7:
Let us denote by w^{lrc} the vector of highest dgree coefficient in $w(x) \in \mathbb{Z}_n^q[X]$, Let $M = p - vect(v_1(x),\ldots,v_k(x))$ be a submodule of $\mathbb{Z}_n^q[X]$. The family $(v_1(x),\ldots,v_k(x))$ is called a p-reduced basis of M if $v_1^{lrc},\ldots,v_k^{lrc}$ p-linearly independent in $\mathbb{Z}_n^q$.
As shown in section 2, every submodule of $\mathbb{Z}_n^q[X]$ can be decomposed into a direct sum of submodules.

Theorem 2:
Every submodule M of $\mathbb{Z}_n^q[X]$ can be written as

$$M = \bigoplus_{i=1}^{m} M_i,$$

where M_i is a submodule of $\mathbb{Z}_n^q[X]$ spanned by a p_i-reduced basis.
From this decomposition can be derived the $(p_1,\ldots,p_m)$-predictable degree proprety, as expressed in the following theorem.

Theorem 3:
Let M be a submodule of $\mathbb{Z}_n^q[X]$; write $M = \oplus_{i=1}^m M_i$ where for all $i = 1,\ldots,m$ the module M_i affords a p_i-reduced basis $(v_1^i(x),\ldots,v_{k_i}^i(x)) \subset \mathbb{Z}_n^q[X]$. Pick $v(x) \in M$. If d denote $rowd(v(x))$ and d_j^i denote $rowd(v_j^i)$ for all $i = 1,\ldots,m$ and $j = 1,\ldots,k_i$ then $v(x)$ can be written in a unique way as:

$$v = \sum_{i=1}^{m}\sum_{j=1}^{k_i} a_j^i(x)v_j^i(x),$$

where for all $i = 1,\ldots,m$, $j = 1,\ldots,k_i$, the quantity $a_j^i(x)$ is a polynomial with coefficients in $\{0,\ldots,p_i-1\}$ and $d^\circ(v_j^i(x)) \leq d - d_j^i$.

Proof. The decomposition $v(x)$ is clearly unique.
If $v_i(x) = \sum_{j=1}^{k_i} a_j^i(x)v_j^i(x)$ then $v_i(x) \in M_i = p - vect(v_1^i(x),\ldots,v_{k_i}^i(x))$, and the same proof as in [1] carries over to show that $d^\circ a_j^i(x) \leq d - d_j^i$ □

IV. Parametrization of behavior annihilators

Definition 8:

Let $R(x)$ be a matrix of $\mathbb{Z}_n^{q\times k}[X]$. Denote by $d_1,\ldots,d_k$ its row degrees.

1) the matrix $R(x)$ satisfies the $p-$predicted degree property iff for all polynomial vector $a(x) = (a_1(x),\ldots,a_k(x))$ with coefficients in $\{0,1,\ldots,p-1\} \subset \mathbb{Z}_n$ the row degree of $a(x)R(x)$ is exactly

$$\max_{1\leq i\leq k}(d_i + dega_i).$$

2) the matrix $R(x)$ satisfies the $(p_1,\ldots,p_k)$-predicted degree property iff there are integers $k_1,\ldots,k_m$ with $k_1 + \ldots + k_m = k$ such that the matrix of the first k_1 rows of $R(x)$ satisfies the p_1-predicted degree property, and so on for the k_2 following rows up to the k_m last rows of $R(x)$.

Definition 9:
Let $R(x)$ be a matrix of $\mathbb{Z}_n^{q\times k}[X]$.

1) $R(x)$ is said to be $p-$reduced, iff the rows of the matrix of highest degree coefficients are $p-$linearly independent in $\mathbb{Z}_n^q$.
2) $R(x)$ is said to be $(p_1,\ldots,p_m)$-reduced iff there are integers $k_1,\ldots,k_m$, $k_1+\ldots+k_m = k$ such that the matrix of the k_1 first rows of $R(x)$ is p_1-reduced, and so on for the k_2 following rows up to the k_m last rows of $R(x)$.

The next theorem connects the $(p_1,\ldots,p_m)$-predicted degree proprety with $(p_1,\ldots,p_m)$–row reduced.

Theorem 4:
Let $R(x)$ be a matrix of $\mathbb{Z}_n^{q\times k}[X]$. It satisfies the $(p_1,\ldots,p_k)-$predicted degree property iff it is $(p_1,\ldots,p_k)$-reduced.

Definition 10:
Let $R(x)$ be a matrix of $\mathbb{Z}_n^{q\times k}[X]$. It is said to be in composed form a permutation matrix P such that the rows of $PR(x)$ are $(p_1,\ldots,p_m)$-generating, that is, iff there are integers $k_1,\ldots,k_m$ with $k_1+\ldots+k_m = k$, such that the k_1 first rows are p_1-generating, the k_2 folllowing rows are p_2-generating, etc, down to the k_m last rows that are p_m-generating.

Theorem 5:
Let B be a behavior given by $R(\sigma)w = 0$, with $R(x) \in \mathbb{Z}_n^{k\times q}$ in composed form (with integres $k_1,\ldots,k_m$ such that $k_1 + \ldots + k_m = k$) and satisfying the $(p_1,\ldots,p_m)$-predicted degree property. Denote by $d_1,\ldots,d_k$ the row degrees of $R(x)$. Let $V(x)$ a polynomial vector of $\mathbb{Z}_n^q[X]$ of row degree d . It is an annihilator of B iff there is a vector $Q(x) = (q_1^1(x),\ldots,q_{k_1}^1(x),\ldots,q_1^m,\ldots,q_{k_m}^m)$ in $\mathbb{Z}_n^k[X]$ such that

1) $V(x) = Q(x)R(x)$.
2) $d^\circ q_i(x) \leq d - d_i$ for $i = 1\ldots,k$.

3) the coefficients of $q_j^i(x)$ are in $\{0, \ldots, p_i\}$ for $j = 1, \ldots, k_i$, $i = 1, \ldots, m$.

In the next theorem we see that every behavior that can be represented by a kernel representation admits a $(p_1, \ldots, p_m)$-row reduced kernel representation in composed form.

Theorem 6:

If B is a behavior on $\mathbb{Z}_n$then there is a kernel representation $R(\sigma)w = 0$ of B such that $R(x)$ is in composed form.

V. Conclusion

This work is a generalization of the paper [1] for semi simple rings. We prove that any submodule M of $\mathbb{Z}_n^q$ can be decomposed into a direct sum of submodules M_i of $\mathbb{Z}_n^q$ which can be spanned by a p_i-generating family. From this decomposition we derive a generalization of all results in [1].

The results in this work are relevant to coding theory, in particular for convolutional codes.

References

[1] Margeretta Kuijper, Raquel Pinto, Jan William Polderman The predictable degree proprety and row reducness for systems over a finite ring. *Linear Algebra and its Applications*, 425 (2007) 776-796.

[2] V.V.Vazirani, H. Saran, B.S. Rajan, An efficient algorithm for construcing minimal trellises for codes over finite abelian groups. *IEEE Trans. Inf. Th.* 42 (1996) 1839-1854.