De Bruijn Digraphs and Affine Transformations

Workshop on Group Theory and Combinatorics
Jeju Island, Korea

Yaokun Wu
Shanghai Jiao Tong University, Shanghai, China
June 22, 2006

- Lots of work in algebraic combinatorics are concerned with the structure and characterizations of (di)graphs defined in some algebraic way. The main result we want to show you in this talk is that a large class of digraphs arising from a general (linear) algebraic construction are closely related to the De Bruijn digraphs.

- Due to the common flavor,we will begin with some beautiful results on linear finite dynamical system, which we learn from a talk of Reinhard Laubenbacher. Indeed, we steal some of his slides here.

- We will end with a brief introduction of some symmetry property of De Bruijn digraphs. This may help convince you that De Bruijn digraphs do play some special role and thus the recognition of them in our algebraic construction may not be so surprising.

Outline

0. Linear finite dynamical system

1. Transformation coset psudo-digraph

2. De Bruijn-like digraphs

3 Affine TCP digraphs

4. Invertible affine TCP digraphs

5. Nonlinear transformations and B(*d*,*n*)

6. More characterizations of B(d,n)

Joint work with Aiping Deng,
Donghua University, Shanghai, China

0. Linear Finite Dynamical System

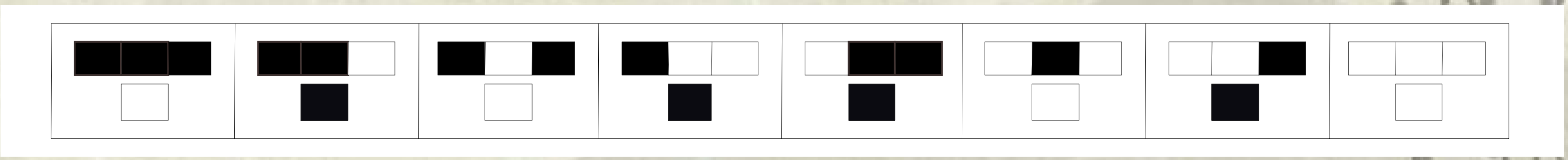
- A Finite Dynamical System (FDS) is a pair (X,f) where X is a finite set and f is a map from X into itself. The dynamics of (X,f) refers to the behavior of f's iterates. In other words, the self-map f defines the time evolution of the system.
- FDS is a useful mathematical model for systems of interacting units and has been studied in theory of finite fields, electrical circuits, neuronal networks, and genetic networks.

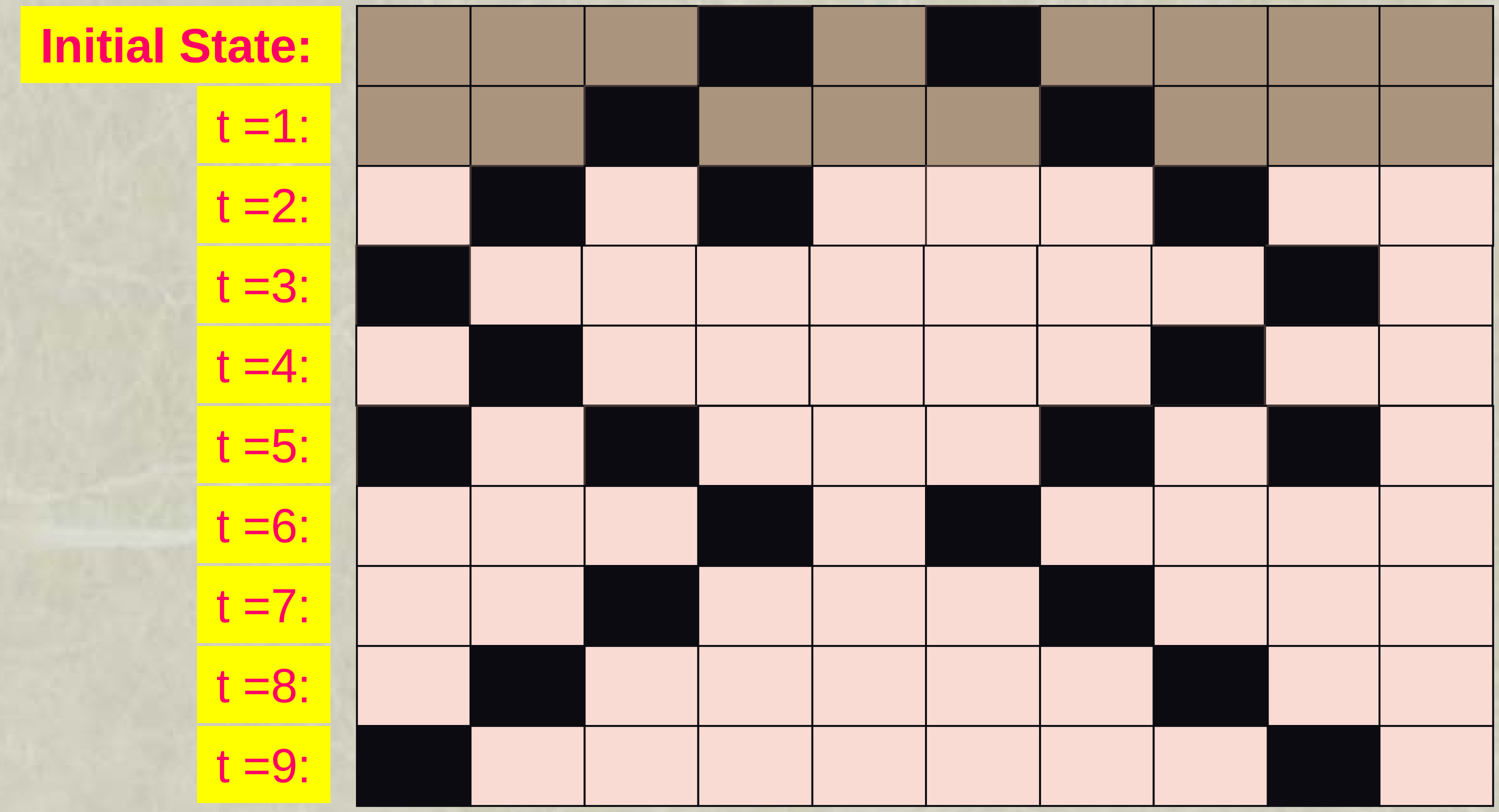
- Both linear FDS and various kinds of nonlinear FDSs are studied in various fields.

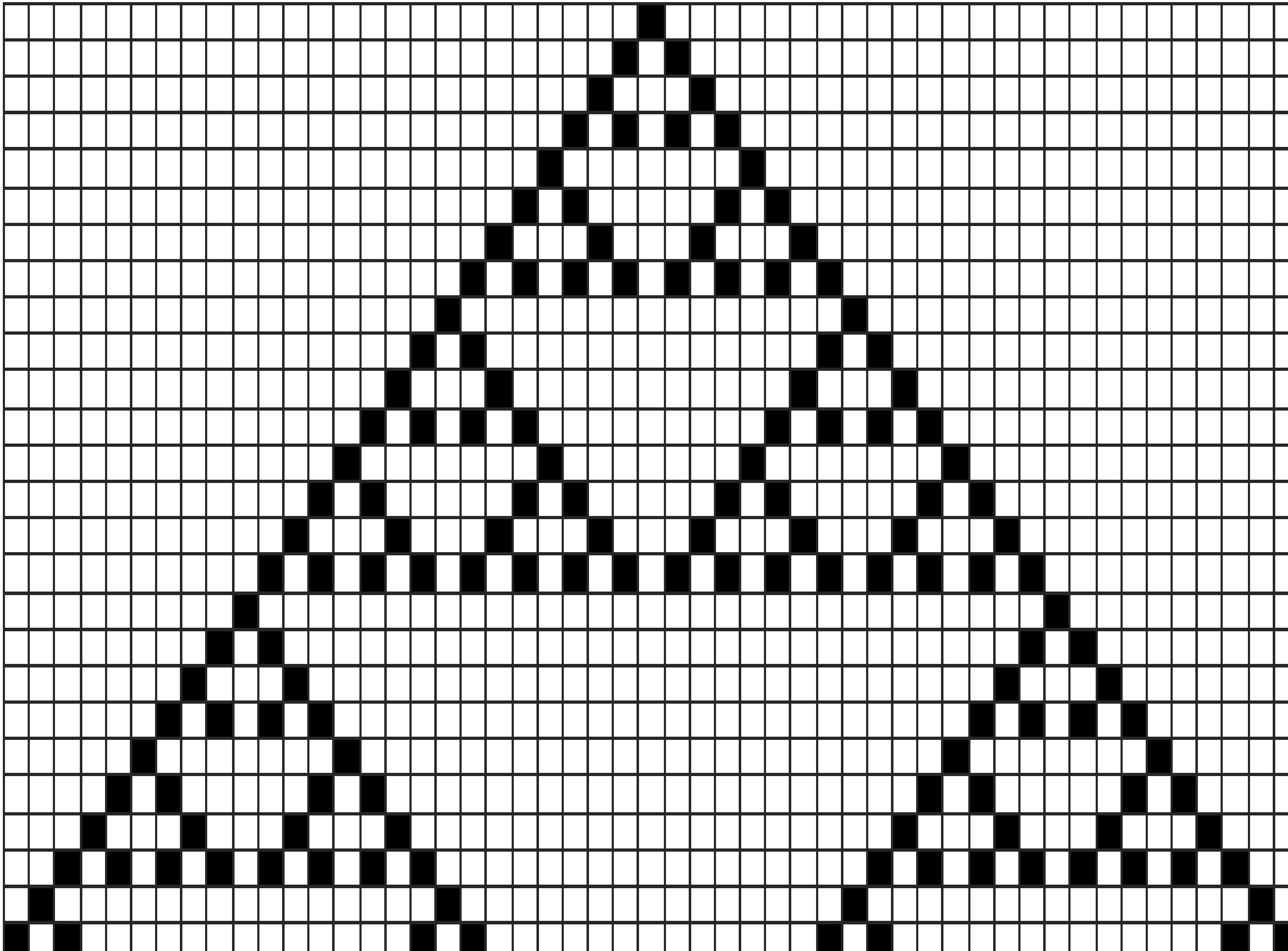
- R.A. Hernandez-Toledo, Linear finite dynamical systems, Communications in Algebra, 33 (2005), 2977—2989.

- A Linear Finite Dynamical System (LFDS) is a pair (X,f), where X is a finite dimensional space over a finite field and f a linear mapping of X into itself. Additive 1-dim cellular automata are important examples of LFDS.

Rule 90 Additive Cellular Automaton







Graphical Representation of Dynamics

The phase space of an FDS $f : X \to X$
is the 1-out regular digraph with vertices the elements of X and there is an edge directed from a to b if and only if $f(a)=b$.

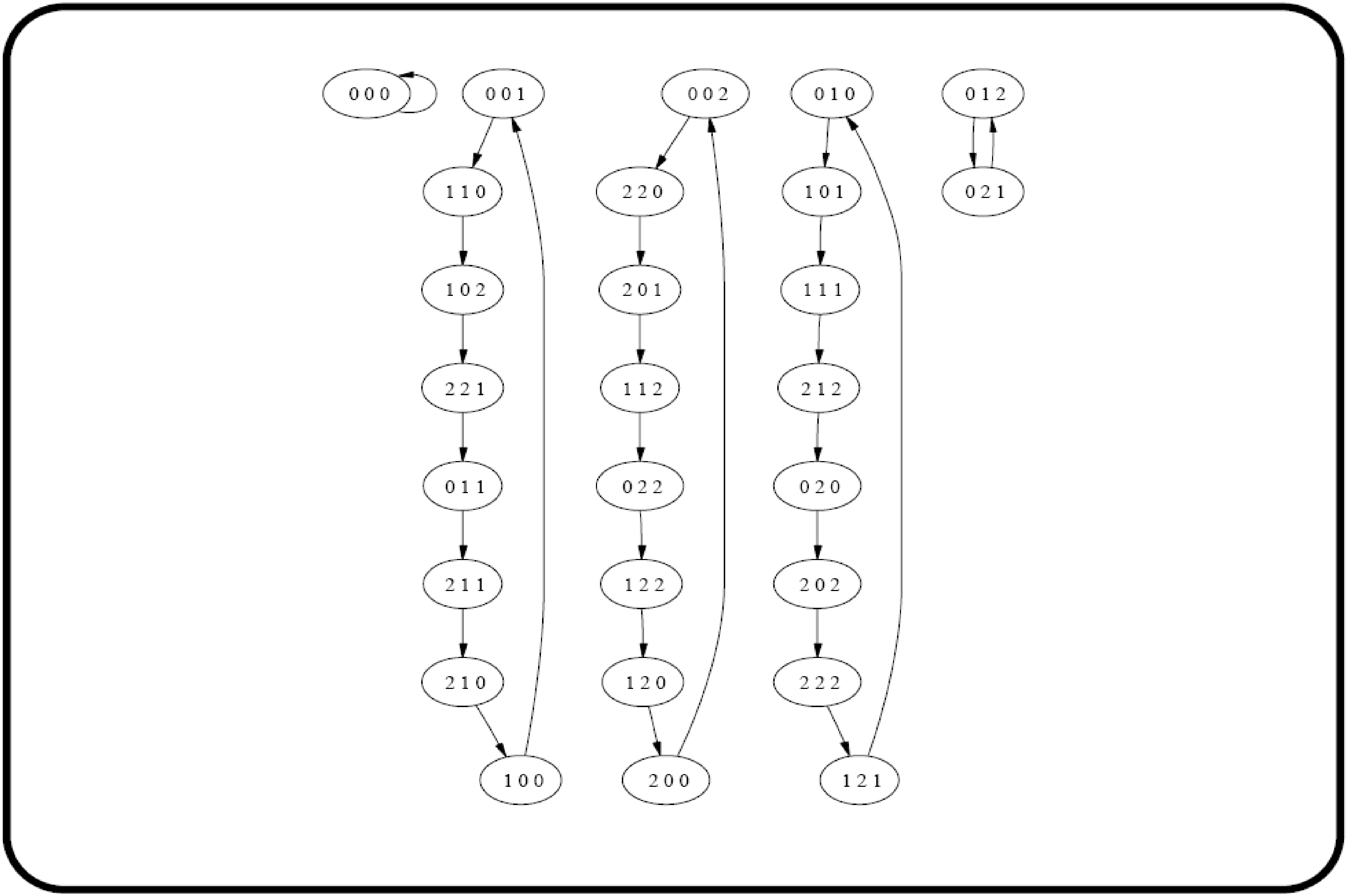
A point is periodic if and only if it lies in a cycle of the phase space.

Question. Can we analyze the dynamics of f without enumerating all phase transitions?

Example: Let $f = (f_1, f_2, f_3) : (\mathbb{F}_3)^3 \longrightarrow (\mathbb{F}_3)^3$, where

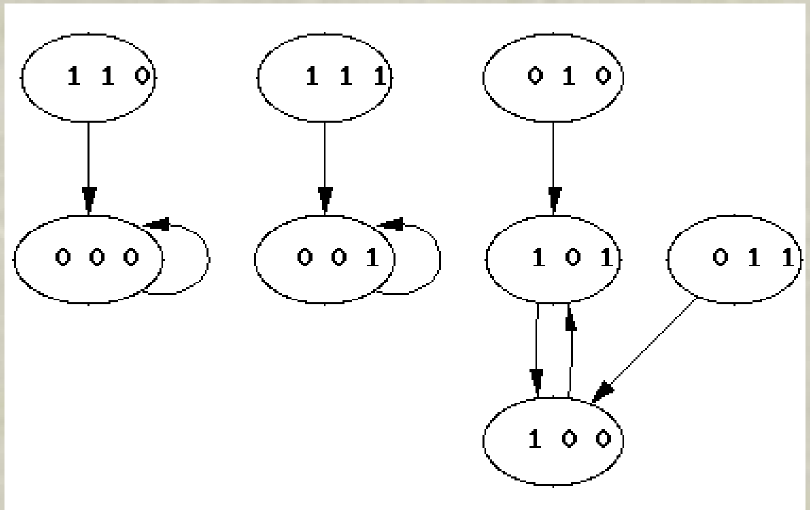
$$\begin{aligned} f_1 &= x_2 + x_3 \\ f_2 &= x_3 \\ f_3 &= x_1 + x_2 \end{aligned}$$

$$f\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}\right) = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}.$$


0 0 0
0 0 1
0 0 2
0 1 0
0 1 2
1 1 0
2 2 0
1 0 1
0 2 1
1 0 2
2 0 1
1 1 1
2 2 1
1 1 2
2 1 2
0 1 1
0 2 2
0 2 0
2 1 1
1 2 2
2 0 2
2 1 0
1 2 0
2 2 2
1 0 0
2 0 0
1 2 1

Example.

$f = (x+y, 0, x+y+z) : \{0,1\}^3 \to \{0,1\}^3$.



Linear Systems.

Let $f : \mathbb{K}^n \longrightarrow \mathbb{K}^n$ be a linear system, represented by an $(n \times n)$-matrix A.

Theorem. (Elspas, Hernandez, Milligan and Wilson,....) The number of components of the phase space, the length of each limit cycle, and the tree structure of the transients can be determined from the factorization of the elementary divisors of A together with the number of field elements. In particular, the structure of the tree of transients at each point in each limit cycle is identical generic tree and completely determined by the algebraic degree of the eigenvalue zero.

Corollary. (Wolfram, Martin, Odlyzko) For a 1-dimensional additive CA the structure of the tree of transients at every periodic node is identical.

- The results obtained in the study of linear finite dynamical systems reveals the regularity of those 1-out regular digraphs which can be the phase space of an LFDS.

- Question: Are there similar results for general D-out regular digraphs?

1. Transformation coset pseudo-digraph

Given an $\alpha \in Z_d^n$ and a transformation F on Z_d^n, the transformation coset pseudo-digraph TCP(Z_d^n, α, F) has the set of cosets of $<\alpha>$ in Z_d^n as vertices and the number of arcs going from $x+<\alpha>$ to $y+<\alpha>$ is # { $z \in x+<\alpha>$: $F(z) \in y+<\alpha>$ }.

TCP(Z_d^n, α, F) is D-out regular where D is the size of $<\alpha>$, namely the order of α.

In the definition of a transformation coset pseudo-digraph TCP(Z_d^n,α, F), if we replace Z_d by some field GF(q), take α =0 and F a linear transformation, then we come back to the phase space of an LFDS.

For any matrix $T \in \mathrm{Mat}_n(Z_d)$ and any row vector $\omega \in Z_d^n$, the affine transformation on Z_d^n w.r.t. T and ω is $F_{T,\omega} : x \to xT+\omega, \forall x \in Z_d^n$.

A vector $\alpha \in Z_d^n$ is a cyclic vector for a linear mapping T provided $< \alpha , \alpha T, \alpha T^2, \ldots > = Z_d^n$. Here, we use $< A>$ for the subgroup generated by A.

Example 1.1 Let $T=\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, α=(0 0 1), ω=(1 0 0). TCP($Z_2^3, \alpha, F_{T,\omega}$) is depicted on the left of Fig. 0. By relablling the vertices as on the right of Fig. 0, we see that it is just the De Bruijn digraph B(2,2).

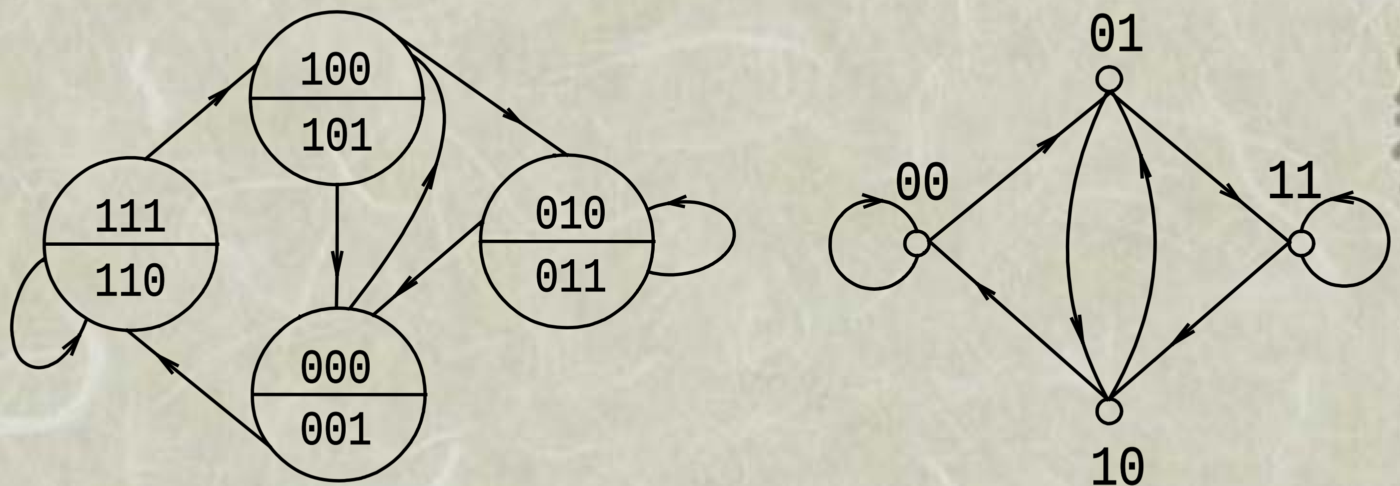


Fig.0 TCP($Z_2^3, \alpha, F_{T,\omega}$) and B(2,2)

2. De Bruijn-like digraph

The d-nary n-dimensional De Bruijn digraph B(d,n) has Z_d^n as its vertex set and there is an arc from ($x_0 x_1 \ldots x_{n-1}$) to ($x_1 \ldots x_{n-1} x_n$) for any $x_i \in Z_d$, $i = 0,\ldots,n$.

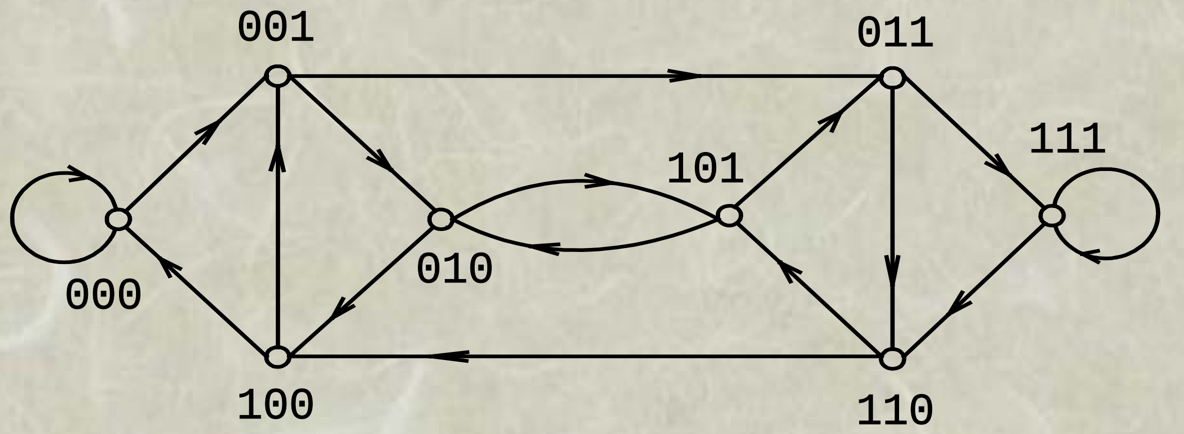


Fig.1 B(2,3)

The r-stage d-nary n-dimensional generalized wrapped butterfly GWBY(r,d,n)=$C_r \otimes B(d,n)$ has vertex set $Z_r \times Z_d^{\,n}$ and there is an arc from (l , $x_0 x_1 \ldots x_{n-1}$) to (l+1, $x_1 \ldots x_{n-1} x_n$) for all $l \in Z_r$ and $x_i \in Z_d$, $i = 0,\ldots,n$.

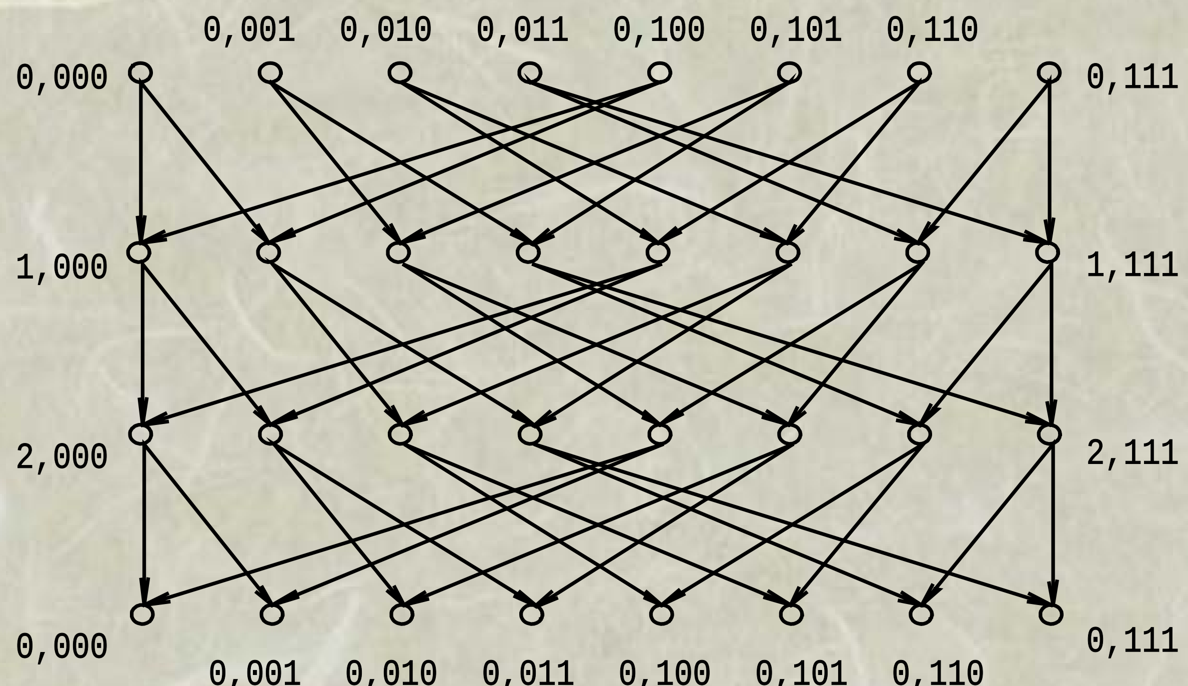


Fig.2 GWBY(3,2,3)= $C_3 \otimes B(2,3)$

The *d*-nary *n*-dimensional multi-wrapped butterfly MWBY(r_1, r_2, ..., r_t; *d*, *n*) is $\cup_{i=1}^{t}$ GWBY(r_i, *d*, *n*), namely a disjoint union of *t* generalized wrapped butterflies.

The r-stage d-nary n-dimensional generalized butterfly GBY(r,d,n)=$P_r \otimes B(d,n)$ has vertex set $[r] \times Z_d^{\,n}$ and there is an arc from (l , $x_0 x_1 \dots x_{n-1}$) to (l+1, $x_1 \dots x_{n-1} x_n$) for all $l \in [r-1]$ and $x_i \in Z_d$, $i = 0,\dots,n$, where $[r]=\{0,1,\dots,r\}$.

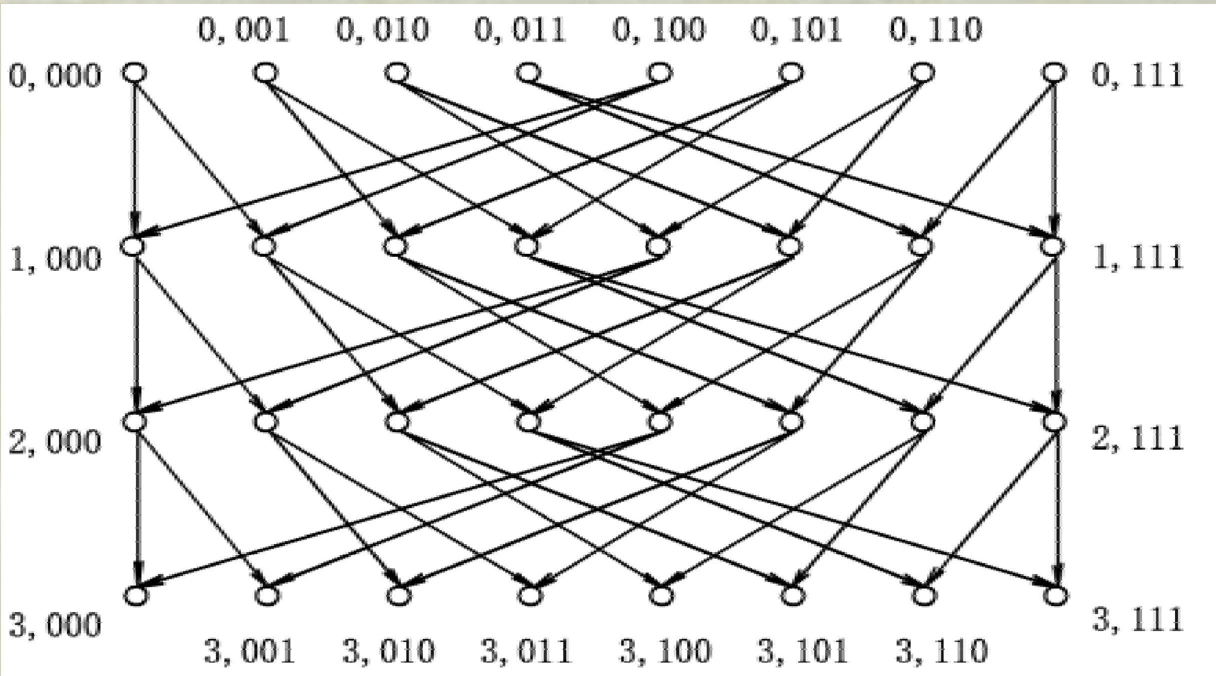


Fig.3 GBY(3,2,3)= $P_3 \otimes B(2,3)$

A digraph Γ is said to be primitive if it is strongly connected and the greatest common divisor of all the cycle lengths of Γ is 1.

3. Affine TCP digraphs

Motivated by their research on nonblocking switching networks, Fiduccia et al. studied the affine TCP digraph representation of De Bruijn digraphs.

C.M. Fiduccia, E.M. Jacobson, Universal multistage networks via linear permutations, in: *Proceedings of the 1991 ACM/IEEE Conference on Supercomputing*, ACM Press, 1991, New York, pp. 380-389.

R.F. Chamberlain, C.M. Fiduccia, Universality of iterated networks, in: *Proceedings of the 4th Annual ACM Symposium on Parallel Algorithms and Architectures*, June 29-July 1, 1992, San Diego, CA, USA. ACM Press, pp. 80-89.

Theorem 3.1 [Fiduccia and Jacobson] For any $T \in GL_n(Z_2)$ and any $\alpha \in Z_2^n$, the following statements are equivalent:

(a) $TCP(Z_2^n, \alpha, F_{T,0}) \cong B(2,n\text{-}1)$;

(b) α is a cyclic vector for T;

(c) The digraph $TCP(Z_2^n, \alpha, F_{T,0})$ is primitive;

(d) The digraph $TCP(Z_2^n, \alpha, F_{T,0})$ is strongly connected;

(e) The digraph $TCP(Z_2^n, \alpha, F_{T,0})$ is connected.

Conjecture 3.2 [Fiduccia and Jacobson]

Let d be a prime number. For any α ,ω $\in Z_d^{\,n}$ and $T \in GL_n(Z_d)$, $TCP(Z_d^{\,n}, \alpha, F_{T,\omega}) \cong B(d,n-1)$ if and only if α is a cyclic vector for T.

Let d and n be two positive integers hereafter. We obtain the following result, which is a strengthening of Conjecture 2.2.

Theorem 3.3 Let $\omega \in Z_d^n$ and $T \in \mathrm{Mat}_n(Z_d)$. For any $\alpha \in Z_d^n$, the following assertions are equivalent:

(a) $\mathrm{TCP}(Z_d^n, \alpha, F_{T,\omega}) \cong \mathrm{B}(d, n\text{-}1)$;

(b) α is a cyclic vector for T;

(c) $\mathrm{TCP}(Z_d^n, \alpha, F_{T,\omega})$ is primitive.

Example 3.4 Let $T=\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, $\alpha=(1\ 0\ 0)$ and $\omega=(0\ 1\ 1)$. TCP($Z_2^3, \alpha, F_{T,\omega}$) ≅ GWBY(2,2,1) is strongly connected but not isomorphic to B(2,2) . This means that (a)<=>(d) part of Theorem 3.1 can not be generalized.

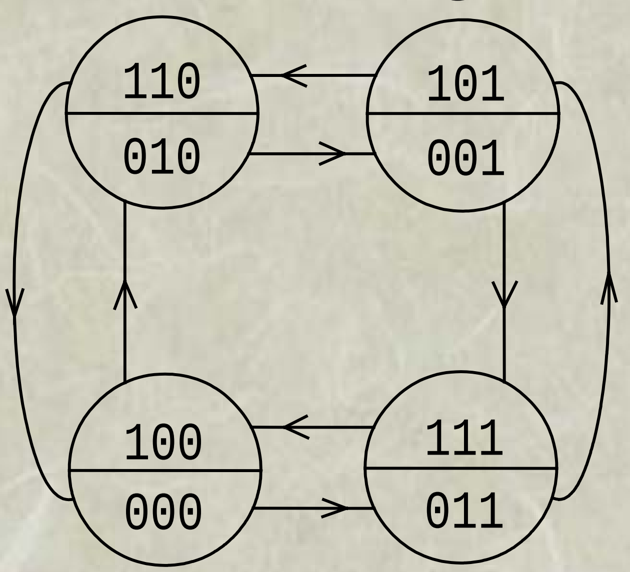


Fig.4 TCP($Z_2^3, \alpha, F_{T,\omega}$) in Example 3.4

Question 3.5 Can we predict the structure of the general affine transformation coset psudo-digraph? We address this question in Section 4.

Question 3.6 What about replacing an affine transformation by a nonlinear transformation? We return to this in Section 5.

Question 3.7 What about replacing Z_d^n by a general module, say GF(q)?

4. Invertible affine TCP digraphs

Theorem 4.1 The digraph TCP($Z_d^n, \alpha, F_{T,\omega}$) with $T \in GL_n(Z_d)$ is a d_0-nary n_0-dimensional multi-wrapped butterfly MWBY(r_1 , r_2 ,…, r_t ; d_0 , n_0), where $d_0 = \#<\alpha>$ and $n_0+1 = \min \{ k>0 : \alpha T^k \in <\alpha T^{k-1}, \ldots, \alpha T, \alpha> \}$.

Question 4.2 What can be said about t, r_1 , r_2 ,…, r_t ? *Note that when* $\alpha=0$, the digraph becomes a union of cycles and the theory of LFDS says something on these parameters.

Example 4.3 Let $T=\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $\alpha=(2\ 0)$, $\omega=(0\ 0)$. $TCP(Z_4^2,\alpha,F_{T,\omega}) \cong$ MWBY(1,3;2,1), which has two components, one being B(2,1), the other being GWBY(3,2,1).

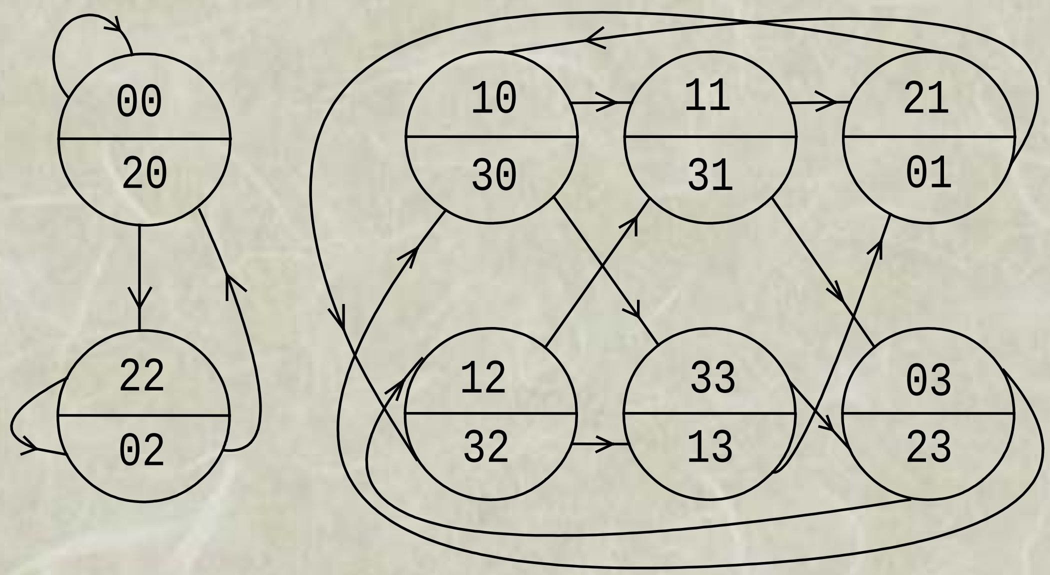


Fig.5 $TCP(Z_4^2,\alpha, F_{T,\omega})$ in Example 4.3

Corollary 4.4 For any α, $\omega \in Z_d^n$ and $T \in GL_n(Z_d)$, the digraph $TCP(Z_d^n, \alpha, F_{T,\omega})$ is strongly connected if and only if it is connected.

This generalizes the (d)<=>(e) part of Theorem 3.1.

Example 4.5 Let $T=\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \notin GL_3(Z_2)$, α=(1 0 0), ω=(0 0 0). TCP($Z_2^{\,3}, \alpha, F_{T,\omega}$) is connected but not strongly connected. This means that the (e)=>(d) part of Theorem 3.1 does not generalize to singular matrices.

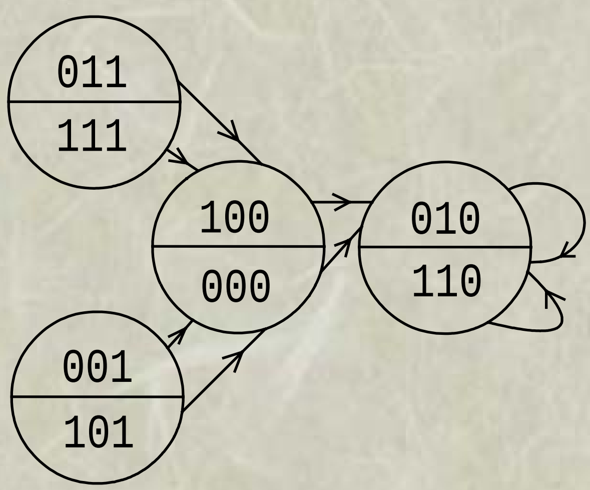


Fig.6

TCP($Z_2^{\,3}, \alpha, F_{T,\omega}$)
in Example 4.5

5. Nonlinear transformations and De Bruijn digraphs

In their work on designing efficient OTIS layouts of De Bruijn networks, Coudert et al. proposed two families of digraphs, $A(g,\pi, j)$ and $H(p,q,d)$, and discussed their uses as representations of De Bruijn-like digraphs.

D. Coudert, A. Ferreira, S. Perennes, Isomorphisms of the De Bruijn digraph and free-space optical networks, *Networks* 40 (2002), 155-164.

Write S_m for the symmetric group on Z_m .

Let $g \in S_n$ and $\pi \in S_d$. The transposition F_g induced by g and the substitution $\beta_{\pi,n}$ induced by π are two permutations on Z_d^n given by

$$F_g((x_0\, x_1\, \dots\, x_{n-1}))=(x_{g(0)}\, x_{g(1)}\, \dots\, x_{g(n-1)})$$

and

$$\beta_{\pi,n}((x_0\, x_1\, \dots\, x_{n-1}))=(\pi(x_0)\, \pi(x_1)\, \dots\, \pi(x_{n-1})),$$

respectively.

Let $e_0, e_1, \ldots, e_{n-1}$ be the standard basis of Z_d^n .

For any $j \in Z_n$, $\pi \in S_d$ and $g \in S_n$, the digraph $\Gamma = A(g, \pi, j)$ is defined by $V(\Gamma) = Z_d^n$, and there is an arc from x to y if and only if $y \in \beta_{\pi,n}(F_g(x)) + <e_j>$.

Example 5.1 If $g \in S_n$ satisfies $g(i) = i+1$ and $\pi \in S_d$ is the identity permutation, then $A(g, \pi, n-1) = B(d,n)$.

For $g \in S_n$, set T_g to be the permutation matrix satisfying $F_g(x) = xT_g$ for every $x \in Z_d^n$.

Fix below $T = \begin{pmatrix} T_g & 0 \\ e_j & 1 \end{pmatrix} \in \mathrm{GL}_{n+1}(Z_d)$.

Let $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_n$ be the standard basis of Z_d^{n+1}.

Lemma 5.2

$\mathrm{TCP}(Z_d^{n+1}, \varepsilon_n, \beta_{\pi,n+1} \bullet F_{T,0}) \cong \mathrm{A}(g, \pi, j)$.

Note that $\beta_{\pi,n+1}$ is not an affine transformation in general.

Theorem 5.3 The following statements are equivalent:

(a) $\mathrm{TCP}(Z_d^{\,n+1}, \varepsilon_n, \beta_{\pi,n+1} \bullet F_{T,0}) \cong \mathrm{B}(d,n)$;

(b) ε_n is a cyclic vector for T;

(c) The digraph $\mathrm{TCP}(Z_d^{\,n+1}, \varepsilon_n, \beta_{\pi,n+1} \bullet F_{T,0})$ is primitive.

This is a nonlinear counterpart of Theorem 3.3.

Corollary 5.4 [Coudert, Ferreira, Perennes]

$A(g,\pi, j) \cong B(d,n)$ if and only if g is a cyclic permutation in S_n.

In general, for any $\alpha \in Z_d^{n+1}$ and $T \in GL_{n+1}(Z_d)$, even if α is a cyclic vector for T, the digraph $TCP(Z_d^{n+1}, \alpha, \beta_{\pi,n+1} \bullet F_{T,\omega})$ may not be a De Bruijn digraph.

Question 5.5 Can we say any more about $\mathrm{TCP}(Z_d^{n+1}, \alpha, \beta_{\pi,n+1} \bullet F_{T,\omega})$?

The digraph H(p,q,d) has vertex set Z_n , where $n = pq/d$ and there is an arc from x to y if and only if $y = \lfloor 1/d\ ((pq-1)(\lfloor (dx+c)/q \rfloor +1) - p(dx+c)) \rfloor$, $c = 0,\ldots,d-1$.

Example 5.6 If $p= d^a$, $q=d^b$ where a and b are nonnegative integers with $a+b=n+1$, then H(p,q,d)=B(d,n).

Conjecture 5.7 [Coudert et al.] If $B(d,n)$ is isomorphic to an $H(p,q,d)$ for some positive integers p, q and d with $d|pq$, then p and q must be powers of d.

Theorem 5.8 If $B(d,n)$ is isomorphic to $H(p,q,d)$, then both p and q are multiples of d.

6. More characterizations of De Bruijn digraphs

- Theorem 6.1: A d^n by d^n nonnegative integer matrix A is the adjacency matrix of B(d,n) if and only if A^n is the all-ones matrix and rank $(A^{n-1})=d$.

- There are similar rank characterization for wrapped butterflies.

Using line digraph techniques, it is easy to determine the automorphism group of generalized wrapper butterflies and generalized butterflies.

Conjecture 6.2: Among all d-regular digraphs on $d^n n$ vertices which admits a homomorphism to the n-cycle, the wrapped butterfly GWBY(n,d,n) is the unique one having the maximum number of automorphisms.

Our conjecture is motivated by a similar conjecture of Hotzel, which asserts that the generalized butterfly GBY(n,d,n) is the unique most symmetric one among all digraphs having the same basic parameters and possessing a homomorphism to the path of length n.

E. Hotzel, Components and graph automorphisms of standard 2×2-switch Banyan networks, Networks 27 (1996), 53 – 71.

C. E. Praeger, Highly arc transitive digraphs, *Europ. J. Combinatorics* 10 (1989), 281 – 292.

If a digraph possesses `certain symmetry properties', then it must be a generalized wrapped butterfly.

N. Golbandi, A. Litman, Characterizations of generalized butterfly networks, Technical Report CS-2004-10, Dept. Of Computer Science, The Technion, 2004, available at: http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2004/CS/CS-2004-10.pdf

Y. Wu, X. Bao, X. Jia, Q. Li, Graph theoretical characterizations of bit permutation networks, draft version, available at: http://math.sjtu.edu.cn/teacher/wuyk/wbjl1.pdf

Thanks!