INFORMATION AND CONTROL 33, 304–332 (1977)

Interconnection Structure of Injective Counters Composed Entirely of *JK* Flip-Flops

M. DAVIO AND G. BIOUL

M.B.L.E. Research Laboratory, Avenue E. van Becelaere 2, 1170 Brussels, Belgium

Counters whose transition map is a permutation and whose constituting elements are *JK* flip-flops only are investigated in order to trace relationships between the interconnection structure and the state graph.

Some equivalence relations over structure transformations are derived that reduce the number of relevant configurations. Numerical computations based on these structure properties show that no circular counter exists for $n \leqslant 9$.

1. INTRODUCTION

The synthesis of counters plays a central role in applied switching theory. This is clearly due to the various practical applications of counters, ranging from frequency division to synchronization of information processing devices.[1]

The class of counters under scope has been investigated by Manning (1972, 1976) and Pless (1976); it consists of synchronous counters constructed only of *JK* flip-flops. Henceforth "counter" means these counters. This class of counters is rather attractive; when a counter of the class realizes a particular state graph, it may be driven with the highest clock rate and, under some conditions, has the minimum cost and the minimum number of internal connections. Manning's thesis essentially uses an experimental approach but also contains theoretical proofs of some interesting properties. More recently, Pless (1976) revisited the problem from a more mathematical point of view. Her paper presents a matrix characterization of *injective counters*, i.e., of counters the transition map of which is a permutation (each state has one and only one successor and predecessor).

Pless (1976) suggests as an open question the periods of injective nonlinear counters. Manning (1972) conjectures that there is no (necessarily injective) counter with n *JK* flip-flops and period 2^n, $n > 3$. This conjecture is based on experiments showing that there is no such counter for $n = 4, 5$.

The present paper tries to trace the relationships that exist between the interconnection structure of the counter and the properties of its state graph.

[1] For usual terminology, the reader is referred to any textbook on switching theory. See, e.g., Dietmeyer (1971).

ISSN 0019-9958

The injective character of the state graph is precisely one of the properties that may be traced back up to the interconnection structure.

After presenting the required definitions in Section 2, we first turn to the study of counter equivalence. The classical equivalence under the group of complementations and of permutations of the state variables is interpreted in terms of structure transformations. It is furthermore shown that other important structure transformations yield isomorphic state graphs. This kind of property is clearly of importance to cut down the overwhelming number of interconnection structures to be considered.

Section 4 presents a first approach to the interconnection structure of injective counters. That approach is based on the concepts of an independent part (a subcounter that does not receive any information on the state of the remaining part of the counter) and of a totally independent part (an independent part that does not provide the remaining part of the counter with any information upon its own state). It is shown that, in an injective counter, any totally independent part is injective and furthermore that it can only be made up of an injective independent part together with a very simple environment. It is shown furthermore that, if the transition map of the counter is a circular permutation, no proper independent part is allowed.

Section 5 is devoted to a restricted family of counters, namely that of linear counters. We establish necessary and sufficient conditions for these counters to be injective, and also exhibit an isomorphism between these injective counters and the well-known linear autonomous shift-registers. The existence of such an isomorphism allows one to give a complete description of the state graph.

In Section 6, we study in more detail the independent parts in nonlinear injective counters and first obtain the rather unexpected result that the maximum fan-out in such counters is two. From this result on, it is shown that, apart from three pathological cases, the independent parts in nonlinear injective counters all share a common interconnection structure called generalized loop structure.

Finally, Section 7 applies the obtained knowledge to the research of counters the transition map of which is a circular permutation and shows by numerical computations that no such counter exists for $4 \leqslant n \leqslant 9$. Moreover we conjecture that generalized loop-counters have an even number of cycles for $n \geqslant 4$.

2. Definitions and Classification

A JK flip-flop is usually described as a device having two (J_i and K_i) binary inputs, a clock-input C_i for synchronization and two binary outputs denoted y_i and $\bar{y}_i$. At a clock transition the new state, i.e., the new output Y_i, is computed according to Dietmeyer (1971), Phister (1958), and Rudeanu (1974) as

$$Y_i = J_i\bar{y}_i \vee \bar{K}_i y_i . \tag{1}$$

More formally a JK flip-flop may be viewed as an abstract automaton that we describe, with Ginzburg (1968) notations, as the algebraic system

$$A = \langle S, \Sigma, \theta, M, N \rangle,$$

where

$$\Sigma = \{(J, K) \mid J, K \in \{0, 1\}\}$$

is the input alphabet and where

$$S = \theta = \{0, 1\}$$

are the state set and the output alphabet, respectively. An arbitrary state $q \in S$ is encoded by means of the single internal state variable y (appearing in (1)) and is identified with the flip-flop output. The transition map M of the JK flip-flop is described by (1) or by Table I.

TABLE I

$M_{(J,K)}$

$M_{(J,K)}$		(J, K)			
		(0, 0)	(0, 1)	(1, 0)	(1, 1)
q	0	0	0	1	1
	1	1	0	1	0

Similarly, a synchronous counter may also be defined as an abstract automaton whose input alphabet contains a single literal. The transition map of a counter thus reduces to a single transformation of the state set and its graph is made up of a certain number of nonconnected components classically called generalized cycles (Dénes, 1968).

In particular, a counter is an *injective counter* or a *permutation counter* iff its transition mapping is a permutation, i.e., iff its state graph contains only cycles. It is a *circular counter* iff its transition mapping is a circular permutation, i.e., iff its state graph consists of a single cycle of length 2^n.

In the present paper, the term *counter* is used to represent a synchronous interconnection of n JK flip-flops (FF) conventionally denoted FF_0, FF_1,..., FF_{n-1}. This definition precludes the presence of additional gates in the counter. The J and K inputs to FF_i are denoted J_i and K_i, respectively. The state (output) of FF_i is denoted y_i. The input–output behavior of the counter is thus completely described by a mapping

$$\{J_i K_i\} \to \{0, 1, y_j^{(e_j)}\} \qquad (i, j \in \{0, 1, \ldots, n-1\}), \tag{2}$$

where the Boolean exponentiation $a^{(e)}$ is used with its usual meaning:

$$a^{(e)} = a \oplus \bar{e} \qquad (e \in \{0, 1\}). \tag{3}$$

The mapping (2) is usually called the *connection list* of the counter (Manning, 1972; Pless, 1976).

One remarks immediately that the constants 0 and 1 are redundant in the connection list (2). Indeed, the JK flip-flop input equation (1) shows that the values $J_i = 0, 1$ (resp. $K_i = 0, 1$) can be replaced, without modifying the flip-flop behavior, by $J_i = y_i, \bar{y}_i$ (resp. $K_i = \bar{y}_i, y_i$). From now on, we shall thus replace the mapping (2) by its restriction:

$$\{J_i, K_i\} \to \{y_j^{(e_j)}\} \qquad (i, j \in \{0, 1,..., n-1\}). \tag{4}$$

Pless (1976) furthermore forbids all the situations in which a flip-flop reacts upon itself, e.g., $J_i = y_i^{(e_i)}$, but it will turn out in Section 6 that this further restriction is not essential for injective counters. We thus consider, according to (4), that there are exactly $(2n)^{2n}$ counters involving n flip-flops and immediately note that the family of counters under study represents a very small part of the $(2^n)^{2^n}$ possible transition mappings on a set of 2^n states.

Under the constraints (4), the input equation (1) becomes

$$Y_i = y_k^{(e)}\bar{y}_i \vee y_l^{(\bar{h})}y_i. \tag{5}$$

Equation (5) suggests a classification of the flip-flops in a counter according to the values of their control inputs J_i and K_i

(a) if $k = l$, FF_i has a unique predecessor. In this case, the flip-flop is called a *linear flip-flop*, since the next value Y_i may be expressed as a linear combination of the present values y_i and y_k. Furthermore,

(i) if $e = \bar{h}$, the flip-flop acts as a synchronized delay element. It is called a

D flip-flop if $e = 1$,
$\bar{D}$ flip-flop if $e = 0$.

(ii) $e = h$, the flip-flop acts as a synchronized toggle switch. It is called a

T flip-flop if $e = 1$,
$\bar{T}$ flip-flop if $e = 0$.

(b) if $k \neq l$, the flip-flop will be called an F flip-flop. In what follows, we shall frequently use an important property of the JK flip-flop: *if the present state y_i of a JK flip-flop is equal to zero (resp. to one), then, its next state Y_i only depends on J_i (resp. on K_i).* That property is an immediate consequence of Eq. (1).

For this reason the inputs J_i and K_i will sometimes be denoted F_{i0} and F_{i1}, respectively. With that notation, F_{ie} represents the actually efficient control input when $y_i = e$. If furthermore a complete knowledge over the polarities of J_i and K_i is required, we shall also denote the F flip-flop as $F_{i0}^{(e)}F_{i1}^{(h)}$ flip-flop.

The counters may be classified according to the nature of the flip-flops they contain. In particular, a counter entirely made up of linear flip-flops is called a *linear counter* (see Section 5). It will be called *nonlinear counter* when it contains at least one F flip-flop.

3. Equivalence

It has been recalled in Section 2 that the number of counters made up of n flip-flops is $(2n)^{2n}$. The investigation of the properties of counters by exhaustive enumeration techniques is thus practically impossible for $n > 5$. It is thus convenient to define an equivalence relation on the set of counters: two counters are *equivalent* iff they have isomorphic state graphs.

Manning (1972) and Pless (1976) have already noted that counters are equivalent under the group of permutations and complementations of the state variables. The purpose of this section is to study the circuit transformations which correspond to this kind of equivalence and to exhibit other circuit transformations which also yield isomorphic state graphs.

The algebraic concept underlying the above defined equivalence is clearly that of isomorphism of automata. We first briefly recall the formal definitions of homomorphism and of isomorphism. The notations used are those of Ginzburg (1968).

Given the automata

$$A = \langle S^A, \Sigma, \theta, M^A, N^A \rangle \quad \text{and} \quad B = \langle S^B, \Sigma, \theta, M^B, N^B \rangle,$$

the mapping ζ of S^A into S^B is a *homomorphism* of A into B iff, for every $\sigma \in \Sigma$:

$$\begin{aligned} &\text{(i)} && M_\sigma{}^A \zeta = \zeta M_\sigma{}^B, \\ &\text{(ii)}^2 && N^A = \zeta N^B. \end{aligned} \tag{6}$$

If the homomorphism ζ is a bijection, it is an isomorphism.

Clearly, if a set of flip-flops in a counter is replaced by an isomorphic automaton, the resulting counter is isomorphic to the given one. A first elementary application of the concept of isomorphism is given by Theorem 1: this theorem in fact accounts for the isomorphism produced by complementing one of the state variables.

[2] This is the simplified definition of homomorphism in the case of complete deterministic Moore automata, which corresponds to the problem under study.

THEOREM 1. *The input-output behavior of a JK flip-flop is left invariant by a simultaneous crossing of the input and output wires.*

Proof. The input equations (1) for both situations displayed in Fig. 1 are

$$C = Y = a\bar{y} \vee \bar{b}y; \qquad D = \bar{Z} = \bar{b}\bar{z} \vee az. \tag{7}$$

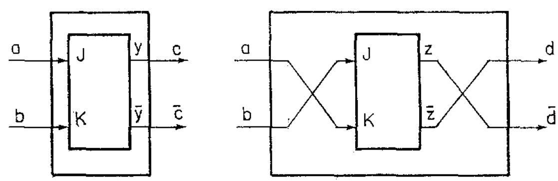

FIG. 1. Crossing the input and output wires of a *JK* flip-flop.

Clearly, the mapping

$$\zeta\colon y \mapsto z = \bar{y} \tag{8}$$

is such that

$$Z = \bar{Y} \quad \text{and} \quad C = D. \qquad \text{Q.E.D.}$$

The practical application of Theorem 1 is straightforward: crossing the input wires of a *JK* flip-flop amounts to complementing all the literals $D^{(e)}$, $T^{(h)}$, $F_0^{(k)}$, $F_1^{(l)}$ corresponding to flip-flop inputs controlled by the modified *JK* flip-flop. The only modification of the code produced is the complementation of the state variable of this flip-flop.

There is no restriction on Theorem 1 and it applies in particular when the *JK* flip-flop is connected as a linear flip-flop:

(a) if the flip-flop is a $T^{(e)}$ flip-flop, crossing the input wires does not change the system: hence, it is allowed to complement simultaneously all the literals $D^{(e)}$, $T^{(h)}$, $F_e^{(k)}$, corresponding to flip-flop inputs controlled by a $T^{(e)}$ flip-flop.

(b) if the flip-flop is a $D^{(e)}$ flip-flop, crossing the input wires amounts to replacing the $D^{(e)}$ flip-flop by a $D^{(\bar{e})}$ flip-flop.

We now consider the cascade connections $A_L = D \ominus A$ and $A_R = A \ominus D$ of a D flip-flop with an arbitrary automaton:

$$A = \langle S^A, \Sigma, \theta, M^A, N^A \rangle; \qquad \Sigma = \theta = \{0, 1\}.$$

The states of A_L and A_R are denoted by (e, q) and (q', e'), respectively. In these pairs e and e' denote states of the D flip-flop, while q and q' denote states of the automaton A (Fig. 2). The transition and output functions of A_L and A_R are denoted by M^L, N^L, M^R, and N^R, respectively.

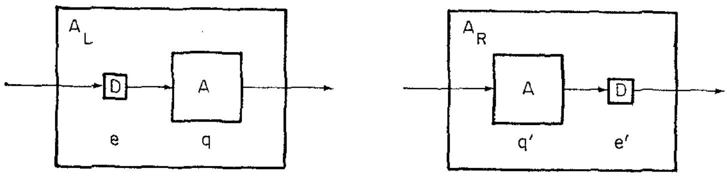

FIG. 2. Cascade connections $A_L = D \ominus A$ and $A_R = A \ominus D$.

LEMMA 1. *The mapping*

$$\zeta\colon (e, q) \mapsto (q', e') = (qM_e^A, qN^A) \tag{9}$$

is a homomorphism of A_L into A_R.

Proof. Clearly,

$$(e, q)M_\sigma^L = (\sigma, qM_e^A) \quad \text{and} \quad (e, q)\, M_\sigma^L \zeta = (qM_e^A M_\sigma^A, qM_e^A N^A).$$

Similarly,

$$(e, q)\zeta = (qM_e^A, qN^A) \quad \text{and} \quad (e, q)\, \zeta M_\sigma^R = (qM_e^A M_\sigma^A, qM_e^A N^A).$$

Furthermore, the output signals are in both cases $qM_e^A N^A$. Q.E.D.

In general, the mapping ζ described in Lemma 1 is not an isomorphism. However, it has that property in some practically important cases to be described in the remaining part of this section.

THEOREM 2. *The cascade connections $D \ominus T^{(h)}$ and $T^{(h)} \ominus D$ of a D and of a $T^{(h)}$ flip-flop are isomorphic.*

Proof. Remember indeed that the input equation of a $T^{(h)}$ flip-flop is

$$Q = q \oplus T \oplus \bar{h}.$$

In that case, the mapping ζ clearly becomes

$$\zeta\colon (e, q) \mapsto (q \oplus e \oplus \bar{h}, q) \tag{10}$$

and is thus one to one. Q.E.D.

A succession of linear flip-flops is called hereafter a *linear cascade*. A linear cascade which only interacts with the external world by the input to the first flip-flop and the output of the last flip-flop is called a *linear string*. In a linear string (Fig. 3), the fan-out of each flip-flop, but the last one, is equal to 1. A linear string is completely characterized by a sequence of literals such as

$$D^{(e_1)} D^{(e_2)} \cdots D^{(e_n)} T^{(h_1)} T^{(h_2)} \cdots T^{(h_p)} D^{(f_1)} \cdots;$$

that sequence is called the *characteristic sequence* of the string.

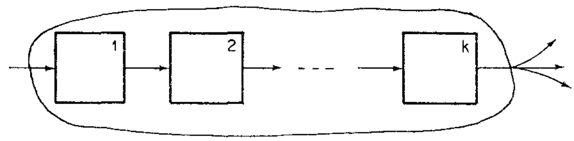

FIG. 3. A linear string.

The application of Theorems 1 and 2 immediately shows that there are only four types of nonequivalent characteristic sequences, namely:

(i) the $D^{(e)}$ *sequence*: $D^{(e)}D\ D \cdots D$,

(ii) the $T^{(e)}$ *sequence*: $D\ D \cdots D\ T^{(e)}T\ T \cdots T \qquad (e \in \{0, 1\})$. (11)

Note that in the $T^{(e)}$ sequence, the substring of D flip-flops may casually be empty. In this case we speak of a *pure* $T^{(e)}$ *sequence.*

We now turn to a second application of Lemma 1 illustrated by Fig. 4. In this case, automaton A consists of an F flip-flop the inputs of which are controlled by pure $T^{(e)}$ sequences.

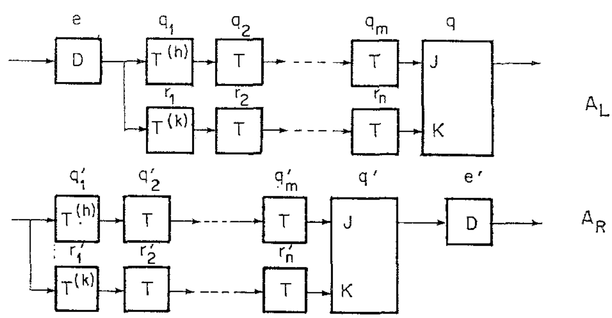

FIG. 4. Two isomorphic automata.

THEOREM 3. *The automata A_L and A_R displayed in Fig. 4 are isomorphic.*

Proof. The homomorphism ζ, introduced by Lemma 1, is described by the equations

$$q_1' = q_1 \oplus e \oplus \bar{h}, \tag{12}$$

$$q_i' = q_i \oplus q_{i-1} \qquad (i = 2, 3,\ldots, m), \tag{13}$$

$$r_1' = r_1 \oplus e \oplus \bar{k}, \tag{14}$$

$$r_j' = r_j \oplus r_{j-1} \qquad (j = 2, 3,\ldots, n), \tag{15}$$

$$q' = \bar{q}q_m \oplus q\bar{r}_n\,, \tag{16}$$

$$e' = q. \tag{17}$$

The mapping ζ will be an isomorphism iff the above system of equations may be solved uniquely for $q_1, ..., q_m, r_1, ..., r_n, q, e$. The discussion considers two cases:

(a) $e' = 0$. In this case, the solution of the system (12)–(17) is unique and is given by

$$q = 0, \tag{18}$$

$$q_m = q', \tag{19}$$

$$q_{i-1} = \left(\sum_{j=i}^{m} q_j' \right) \oplus q', \tag{20}$$

$$e = \left(\sum_{j=1}^{m} q_j' \right) \oplus q' \oplus \bar{h}, \tag{21}$$

$$r_j = \left(\sum_{u=1}^{j} r_u' \right) \oplus \left(\sum_{v=1}^{m} q_v' \right) \oplus q' \oplus h \oplus k. \tag{22}$$

(b) $e' = 1$. This case is handled in exactly the same way as the former one.

If p is some state appearing in the left-hand members of (18)–(22) and if p_0 and p_1 represent the solutions corresponding to the situations $e' = 0$ and $e' = 1$, one finally obtains

$$p = p_0 \bar{e}' \oplus p_1 e'. \tag{23}$$

Q.E.D.

4. Interconnection Structure of Injective Counters

The arguments developed up to now are of a quite general nature since they apply to any counter. From the present section on, we turn to more specialized arguments which progressively reduce our scope to circular counters.

An *independent k-part* of a counter is a set of k flip-flops in the counter each of which is controlled only by some other(s) flip-flop(s) of the set. Thus, an independent part of a counter receives no information about the state of the complementary part of the counter, while it may control some flip-flops in that complementary part. When the complementary part is also an independent part, both parts are *totally independent* or disconnected.

We start by studying the nature of independent parts in injective counters.

LEMMA 2. *A totally independent part of an injective counter is an injective counter.*

Proof. Denote by q_1 and q_2 the states of the two totally independent parts, say P_1 and P_2. Assume that P_1 is not injective. In that case, P_1 has two states, say q_{1a} and q_{1b}, which have the same successor. In that case, both states (q_{1a}, q_2) and (q_{1b}, q_2) of the given counter would also have the same successor and the counter would not be injective. Q.E.D.

From now on, we may thus confine ourselves in the study of injective counters having no proper totally independent part. The second question that arises is naturally that of the presence of (not totally) independent parts. The answer to that question will be provided by Theorem 4. The complementary part of a (not totally) independent part is called the *dependent part.*

LEMMA 3. *An injective counter made up of n flip-flops contains an independent* $(n - 1)$*-part iff the two following conditions simultaneously hold true*:

(i) *The dependent part is a* $T^{(h)}$ *flip-flop.*

(ii) *The independent part is an injective counter.*

Proof. (a) Assume first that the counter is injective and contains an independent $(n - 1)$-part. Denote the state of the counter by (q, e, f) where f is the state of the dependent part, e is the state (or the pair of states) that control the dependent part and q is the state of the remaining part of the counter. If the dependent part is not a $T^{(h)}$ flip-flop, there is always some state of e for which the J and K inputs of the dependent flip-flop receive complementary values. In that case, both states (q, e, x) $(x \in \{0, 1\})$ have the same successor and the counter is not injective. Thus condition (i) holds true. Assume now that the independent part is not injective. In that case, it contains two states (q_1, e_1) and (q_2, e_2) which have the same successor (q, e). Then, the two states of the counter are (q_1, e_1, f_1) and (q_2, e_2, f_2), where

$$f_1 \oplus e_1 = f_2 \oplus e_2$$

would also have the some successor $(q, e, e_1 \oplus f_1)$, since, thanks to (i), the dependent part is a $T^{(h)}$ flip-flop. The counter would not be injective. Thus condition (ii) holds true.

(b) Assume now that both conditions (i) and (ii) hold true. Consider a specific cycle of the state graph of the independent part: assume that this cycle has length l and that, during the cycle, the control bit e of the $T^{(h)}$ flip-flop assumes the value h w times. In the state graph of the counter, we may thus associate two cycles of length l if w is even and one cycle of length $2l$ if w is odd. The counter is thus injective. Q.E.D.

LEMMA 4. *If an independent part of a counter controls a single of the two inputs of an F flip-flop, the counter is not injective* $(n \geqslant 3)$.

Proof. In an injective counter, an F flip-flop never controls a single of its inputs (see Section 6). The only situation to consider is thus described by Fig. 5. The state of the counter is denoted $(\mathbf{q}_1, q_2, q_3, q_4, \mathbf{q}_5)$, where

q_2 is the state of the flip-flop of the independent part that controls a single input of the F flip-flop (say the J input).
$\mathbf{q}_1$ is the state of the rest of the independent part ($(k - 1)$-tuple).
q_3 is the state of the flip-flop that controls the K input of the F flip-flop.
q_4 is the state of the F flip-flop.
$\mathbf{q}_5$ is the state of the remaining part of the counter ($(n - k - 2)$-tuple).

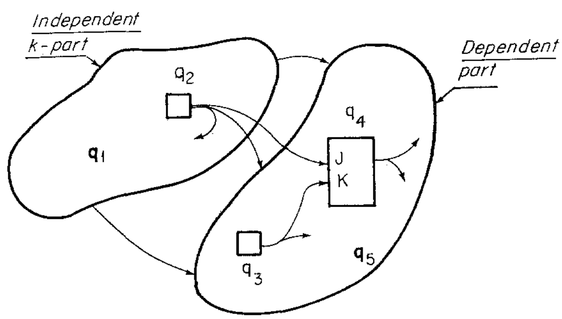

FIG. 5. Illustration of Lemma 4.

Now, for fixed $\mathbf{q}_1$, the $3 \cdot 2^{n-k-2}$ states

$$(\mathbf{q}_1, 0, 0, 0, \mathbf{q}_5), \qquad (\mathbf{q}_1, 0, 1, 0, \mathbf{q}_5), \qquad (\mathbf{q}_1, 0, 1, 1, \mathbf{q}_5) \tag{24}$$

all have their successors among the $2 \cdot 2^{n-k-2}$ states

$$(\mathbf{q}_1', e,-, 0,-),$$

since $\mathbf{q}_1'$ and e are uniquely determined by the independent k-part. Clearly, some of the states mentioned in (24) have common successors. The counter can thus not be injective. Q.E.D.

THEOREM 4. *Any independent k-part of an injective counter is an injective counter. Furthermore, the dependent part is entirely made up of $T^{(h)}$ flip-flops.*

Proof. The proof is by induction on the number p of flip-flops in the dependent part. Lemma 3 provides us with the initial step of the induction $p = 1$ and we thus assume as induction hypothesis that the property holds true for $p = n - k - 1$. Consider now a not totally independent k-part. It controls at least one input to some flip-flop in the dependent part but Lemma 4 then shows that the independent part has to control both inputs to that flip-flop. We may thus form an independent $(k + 1)$-part by adjoining the latter flip-flop to the given independent k-part. The induction hypothesis applies here to show that the obtained independent $(k + 1)$-part is injective and Lemma 3 finally shows that the given independent k-part is injective while the adjoined flip-flop is a $T^{(h)}$ flip-flop. Q.E.D.

Lemma 2 and Theorem 4 indicate the method by which all injective counters are built from smaller injective counters having no proper independent part. These "core" injective counters will be called *simple counters*. The importance of simple counters will be emphasized in Theorem 5, where we show that any circular counter is simple. First we present the counterparts of Lemmas 2 and 3 for circular counters. This is done in Lemmas 5 and 6, respectively.

LEMMA 5. *An independent part of a circular counter is a circular counter.*

Proof. Denote by q_1 the state of the independent part and by q_2 the state of its complement. Assume that the independent part is not circular. Thus it has a state q_{1a} from which it is impossible to reach some other state, say q_{1b}. In that case, it is impossible to pass from the state (q_{1a}, q_2) of the counter to any other state of the form (q_{1b}, q_2'). Q.E.D.

Remark. An immediate consequence of Lemma 5 is that a circular counter cannot be made up of totally independent parts. If k and $(n - k)$ denote the number of flip-flops in two totally independent parts, the counter would have a cycle of length LCM $(2^k, 2^{n-k}) = \max(2^k, 2^{n-k})$.

LEMMA 6. *A circular counter made up of n flip-flops* $(n > 2)$ *does not contain any independent* $(n - 1)$*-part.*

Proof. Assume that there exists an independent $(n - 1)$-part. We know by Lemma 3 that the dependent flip-flop is a $T^{(h)}$ flip-flop and by Lemma 5 that the independent part is circular, i.e., that its state graph has a single cycle of length 2^{n-1}. During the cycle, the $T^{(h)}$ flip-flop receives exactly 2^{n-2} ones; i.e., except for $n = 2$, it changes its state an even number of times and thus returns to its initial state when the cycle is completed. This completes the proof of the lemma. Q.E.D.

Remark. There is only one circular counter with one flip-flop. It consists of a $\bar{D}$ flip-flop looped on itself. When such a flip-flop feeds a T flip-flop, one obtains a binary code counter (Fig. 6). This remark covers the case $n = 2$.

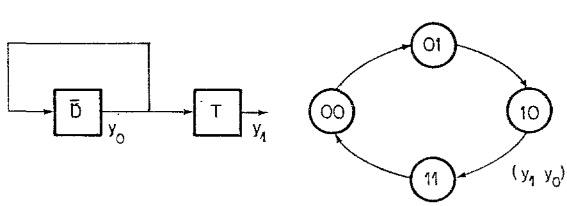

FIG. 6. Pathological case $n = 2$ (binary code).

THEOREM 5. *A circular counter* ($n > 2$) *is simple.*

Proof. The proof rests upon the following observation. If a circular counter contains an independent part, it also contains an independent part that controls a single of the two inputs of an F flip-flop. Indeed, it is possible to enlarge progressively the given independent part while preserving its independent character by augmenting it with all the flip-flops it controls entirely. To avoid the situation forbidden by Lemma 6, this progressive building up has to be stopped somehow; the only way to achieve this result is precisely to control a single of the two inputs to an F flip-flop. However, the latter situation is prevented by Lemma 4. Q.E.D.

Thanks to Theorem 4 and 5, we are now allowed to restrict our scope to simple counters.

5. SIMPLE LINEAR COUNTERS

By definition, linear counters are made up of linear flip-flops only; each of their component flip-flops has a unique predecessor. Simple linear counters are thus *loop-counters*, i.e., linear strings the output of which is recirculated to the input. An elementary application of the isomorphism theorems shows that, in the case of loop-counters, we only have to consider three types of characteristic sequences: the T and $\bar{T}$ sequences are indeed equivalent.

THEOREM 6. *Any loop-counter is injective except when its characteristic sequence is a pure T sequence. In the latter case, two complementary states always have the same successor.*

Proof. We consider (Fig. 7) the case of an arbitrary T sequence containing k T flip-flops and $(n-k)$ D flip-flops. To achieve the proof, we only have to show that no two distinct states have the same successor. We thus consider the states

$$\mathbf{y} = (y_0, y_1, \ldots, y_{n-1}) \qquad \text{and} \qquad \mathbf{z} = (z_0, z_1, \ldots, z_{n-1}).$$

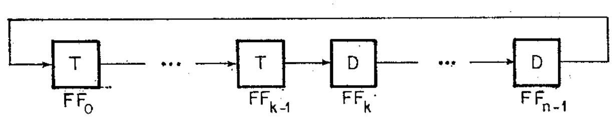

FIG. 7. Loop-counter with a characteristic T sequence.

The equality of their successor states $\mathbf{Y}$ and $\mathbf{Z}$ implies

$$y_0 \oplus y_{n-1} = z_0 \oplus z_{n-1}, \tag{25}$$

$$y_{i-1} \oplus y_i = z_{i-1} \oplus z_i \qquad (i = 1, 2, \ldots, k-1), \tag{26}$$

$$y_{j-1} = z_{j-1} \qquad (j = k, k+1, \ldots, n-1). \tag{27}$$

This system of equations has the unique solution $y_i = z_i$ $(i = 0, 1,..., (n - 1))$ if $k < n$; i.e., if there is at least one equation of type (27). If $k = n$ (pure T sequence), the above system also has the solution $y_i = \overline{z_i}$ $(i = 0, 1,..., (n - 1))$. Finally, if the characteristic sequence is a $D^{(e)}$ sequence, all the equations are of form (27) and the property is trivial. Q.E.D.

THEOREM 7. *Except for $n = 2$, no loop counter is circular.*

Proof. Indeed, in all the counters the characteristic sequence of which is a D or a T sequence, the all–zero state is its own successor state. When the characteristic sequence is a $\bar{D}$ sequence (switch-tailed register (Manning, 1972)), all the cycle lengths divide $2n$. For $n = 2$, one obtains a well-known Gray-code circular counter (Fig. 8). Q.E.D.

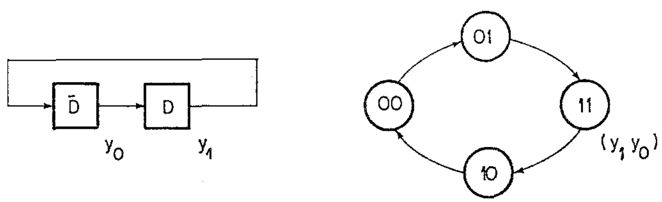

FIG. 8. Gray-code loop-counter ($n = 2$).

In what follows, we investigate the cycle structure of the transition graph of injective linear counters. More precisely, we establish an isomorphism between the loop-counter displayed in Fig. 7 and the classical linear autonomous shift-register (Elspas, 1959) (Fig. 9). We shall then be in position to apply to our loop-counters the results available about linear autonomous shift registers.

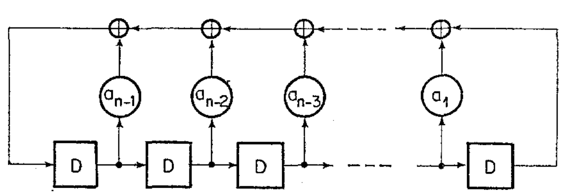

FIG. 9. Autonomous linear shift-register.

The next state equations related to the counter of Figs. 7 and 9 may be written, respectively, under the matrix form

$$[Y] = [B][y], \tag{28}$$

$$[Z] = [C][z], \tag{29}$$

where the matrix product is computed over GF (2). Matrices $[B]$ and $[C]$ are easily derived from Figs. 7 and 9, respectively, while $[Y]$, $[y]$ (resp. $[Z]$, $[z]$) are the corresponding state vectors. In the present context, an isomorphism between the two linear systems is defined by a regular matrix $[M]$ such that one has simultaneously

$$[z] = [M][y], \tag{30}$$

$$[Z] = [M][Y]. \tag{31}$$

It is known (Elspas, 1959) that the above relations are equivalent to similarity of matrices $[B]$ and $[C]$ under the transformation by $[M]$,

$$[C] = [M][B][M]^{-1}, \tag{32}$$

which implies in turn the equality of characteristic polynomials $\phi(B)$ and $\phi(C)$. Since one has

$$\phi(B) = (1 \oplus \lambda)^k \lambda^{n-k} \oplus 1 \tag{33}$$

and

$$\phi(C) = \lambda^n \oplus \sum_{j=1}^{n-1} a_j \lambda^j \oplus 1, \tag{34}$$

the coefficients a_j are uniquely determined as

$$a_j = \binom{k}{n-j}_2 \qquad (j = 1, 2, \ldots, n-1), \tag{35}$$

where binomial coefficients are computed modulo 2 and where

$$\binom{a}{b} = 0 \qquad \text{whenever } b < 0 \text{ or } b > a. \tag{36}$$

Thus, $a_j = 0$ if $j < n - k$.

We now define the $[M]$ matrix as

$$[M] = \left[\begin{array}{c|c} \tilde{M} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{1} \end{array}\right], \tag{37}$$

where $\mathbf{1}$ is a unit matrix of order $(n - k)$ and where $\tilde{M}$ is a square matrix of order k, the rows and columns of which are numbered from 0 to $(k - 1)$ and the (i, j) entry of which is defined by

$$\tilde{m}_{ij} = \binom{k-i-1}{j-i}_2. \tag{38}$$

Since $m_{ij} = 0$ if $j < i$, the matrix $[M]$ defined by (37) and (38) is upper triangular and clearly regular.

THEOREM 8. *The loop-counter of Fig. 7 and the autonomous linear shift-register are isomorphic under the transformation* $[M]$.

The proof of Theorem 8 is purely computational and has not been presented here, since it is rather tedious. The importance of Theorem 8 is due to the fact that it allows one to derive the complete cycle structure of the state graph of a loop-counter from its characteristic polynomial $\phi(B)$. In particular,

(i) if the characteristic polynomial $\phi(B)$ is primitive, there exist a cycle of length 1 and a cycle of length $2^n - 1$;

(ii) if the polynomial $\phi(B)$ is irreducible and if k is the smallest integer such that $\phi(B)$ divides $(\lambda^k \oplus 1)$, there exist a cycle of length 1 and $(2^n - 1)/k$ cycles of length k;

(iii) if the polynomial $\phi(B)$ is not irreducible, the cycles of the state graph are in general of unequal length (for more detailed results, see Elspas, 1959).

Characteristic polynomials $\phi(B)$ may be checked for primitive and/or irreducible character in classical tables such as the one of Peterson (1961).

The limitations of the loop-counters clearly appear when one notices that no $\phi(B)$ is primitive for $n = 8$ and $n = 12$.

6. SIMPLE INJECTIVE NONLINEAR COUNTERS

The present section completes the study of injective counters by showing that, apart from three pathological cases corresponding to $n = 3$, all the simple injective nonlinear counters share a common interconnection structure. Lemmas 7 and 8 first exhibit some structures that are forbidden in injective counters.

LEMMA 7. *If, in a counter, a* $D^{(e)}$ *flip-flop only controls single inputs to* F *flip-flops, the counter is not injective.*

Proof. The situation under discussion is sketched in Fig. 10. We assume that the $D^{(e)}$ flip-flop controls the input F_{ie_i} to the F flip-flop FF_i. The state of the counter is denoted by

$$(y_0, y_1, \ldots, y_p, \mathbf{y}),$$

where

y_0 is the state of the $D^{(e)}$ flip-flop,
$y_1 \cdots y_p$ are the states of the F flip-flops,
$\mathbf{y}$ is the state of the remaining part of the counter.

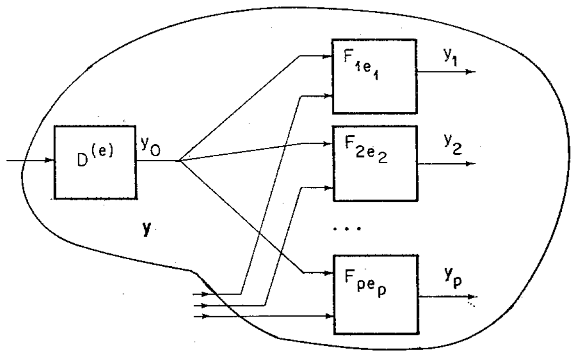

FIG. 10. First situation forbidden in an injective counter.

Note that the successor state of $\mathbf{y}$ only depends on $y_1, \ldots, y_p$ and $\mathbf{y}$ but not on y_0. Furthermore, if $y_i = \bar{e}_i$ its successor only depends on $F_{i\bar{e}_i}$ and thus not on y_0. Thus the two states

$$(x, \bar{e}_1, \bar{e}_2, \ldots, \bar{e}_p, \mathbf{y}); \qquad (x \in \{0, 1\})$$

have the same successor and the counter is not injective. Q.E.D.

LEMMA 8. *If, in a counter, a JK flip-flop FF_0 only controls single inputs to F flip-flops along linear strings and if, furthermore, it is simultaneously possible to choose the states y_i of the F flip-flops so as to make their next states independent of y_0 and to apply complementary values to the control inputs of FF_0, the counter is not injective.*

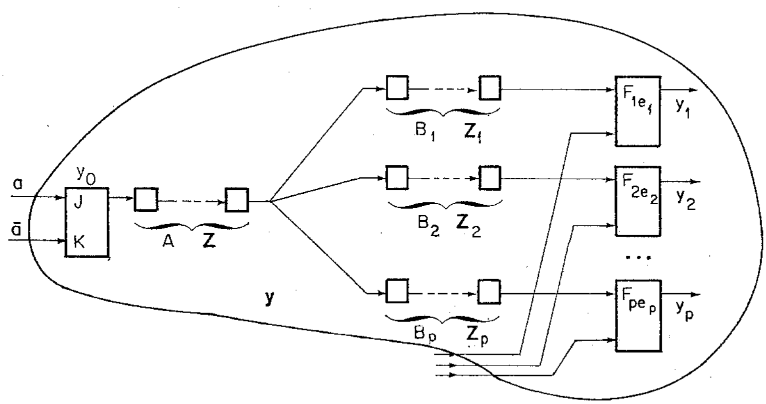

FIG. 11. Second situation forbidden in an injective counter.

Proof. The situation under discussion is displayed in Fig. 11. One first notes that the strings $B_1, \ldots, B_p$ are only made up of $T^{(e)}$ flip-flops. Otherwise, the counter would not be injective, as shown by Lemma 7. We may furthermore assume that the string A only contains $T^{(e)}$ flip-flops. Indeed, if A were to contain a $D^{(e)}$ flip-flop, one could choose this flip-flop as FF_0 and the lemma would apply without any restriction since a $D^{(e)}$ flip-flop receives, by definition, complementary inputs. The state of the counter is then denoted by

$$(y_0, \mathbf{z}, \mathbf{z}_1, \ldots, \mathbf{z}_p, y_1, y_2, \ldots, y_p, \mathbf{y}),$$

where the symbols have the same meaning as in Lemma 7 and where furthermore $\mathbf{z}$ and $\mathbf{z}_i$ represent the states of the strings A and B_i, respectively. Finally if $\mathbf{x}$ is a vector all the components of which are equal to x, it becomes elementary to observe that both states

$$(x, \mathbf{x}, \mathbf{x}, \ldots, \mathbf{x}, \bar{e}_1, \bar{e}_2, \ldots, \bar{e}_p, \mathbf{y}); \qquad (x \in \{0, 1\})$$

have the same successor. Q.E.D.

Remark 1. Lemma 8 applies without restriction in many situations. Indeed, it is always possible to satisfy the hypotheses when

(i) FF_0 is a $D^{(e)}$ flip-flop,

(ii) $p = 1$,

(iii) FF_0 is an F flip-flop which is not directly controlled by two of the F flip-flops $y_1 \cdots y_p$.

Remark 2. Another consequence of Lemma 8 is that a simple injective counter cannot contain only $D^{(e)}$ and F flip-flops. Indeed, the only way to avoid the situation forbidden by the lemma is to provide each $D^{(e)}$ flip-flop with at least one successor of the D type: in this case however, the set of $D^{(e)}$ flip-flops forms an independent part and the counter is not simple.

Before turning to the main theorems of this section, we introduce the concept of basic three-pole: a *basic three-pole* is a set of flip-flops that consists of an F flip-flop together with three (possibly empty) linear strings (Fig. 12).

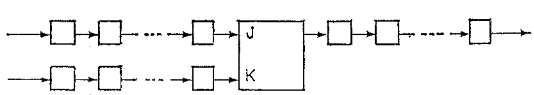

FIG. 12. Basic three-pole.

THEOREM 9. *Each injective simple nonlinear counter (i.s.n.c.) is an interconnection of basic three-poles each of which has a fan-out exactly equal to two. Alternatively, each i.s.n.c. consists of a tree of basic three-poles and a permutation network*

Proof. Assume that the counter contains exactly p F flip-flops. Since the counter is nonlinear, there is at least one flip-flop of that type. Select arbitrarily the J input of one of these flip-flops, say $FF1$, find its predecessor, the predecessor of the J input of the latter, and so on, until the obtained predecessor is an already encountered flip-flop. The same process is then repeated from the remaining K inputs on and finally produces a tree made up of F flip-flops and of possibly empty linear cascades. A typical situation is described by the heavy frame in Fig. 13. Note that the n flip-flops in the counter, and, in particular, the p F flip-flops have been reached by the above process since, by hypothesis the counter is simple. At this stage, there are exactly $(p + 1)$ inputs not yet connected. One notes, however, that the output of $FF1$ has to be connected to one of these inputs, since otherwise there would exist an $(n - 1)$-independent part. This is exemplified by the dotted line in Fig. 13. In the present situation, there are exactly p unconnected inputs while p F flip-flops control a single input to another F flip-flop along a linear cascade. To prevent the situation forbidden by Lemma 8 (Remark 1(ii)) each of these p cascades should be broken down in two strings by some fan-out connection. The circuit may thus only be completed by a permutation box π that connects these p additional outputs to the p unconnected inputs It is then an elementary matter to redraw the circuit of Fig. 13 as an interconnection of basic three-poles each of which has a fan-out equal to 2. Q.E.D.

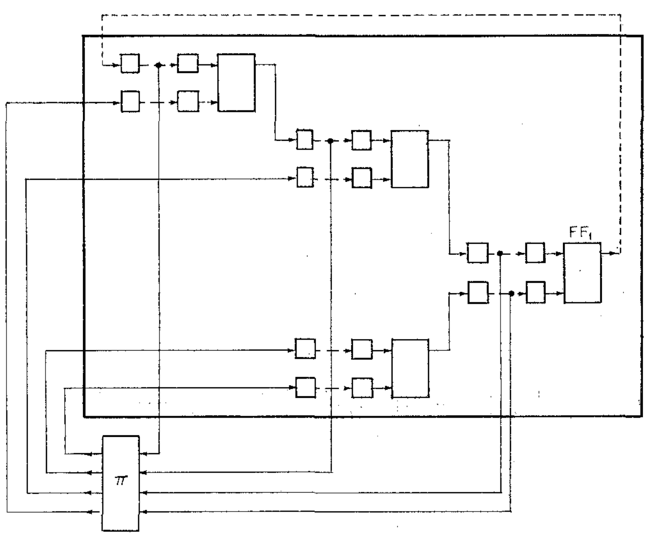

FIG. 13. Illustration of the proof of Theorem 9.

The number of trees and of permutation networks to be considered in constructing injective counters is much lower than suggested by Theorem 9. Lemma 8 has only been used in a very particular case but, when it is used with its full strength, it eliminates a number of structures still covered by Theorem 9. Lemma 9 brings a further reduction in the number of allowable connections.

LEMMA 9. *In an injective simple counter, an F flip-flop never reacts upon a single of its inputs along a linear cascade.*

Proof Thanks to Theorem 9, we may represent the situation under study as displayed in Fig. 14. We note furthermore, thanks to Lemma 8, that none of the strings A, B and C, contains a $D^{(e)}$ flip-flop We discuss two cases.

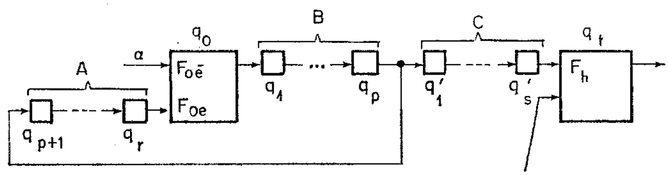

FIG. 14. Third situation forbidden in an injective counter.

(i) The cascade formed by the strings B and A is empty. In this case, if we denote by q_0 the state variable corresponding to the F flip-flop, one has $F_{0e} = q_0^{(k)}$ and the flip-flop input equation, which may be written in general as

$$Q_0 = q_0^{(e)} F_{0e}^{(\bar{e})} \vee q_0^{(\bar{e})} F_{0\bar{e}}^{(e)}, \tag{39}$$

becomes

$$Q_0 = q_0^{(e)} q_0^{(e \oplus k)} \vee q_0^{(\bar{e})} \alpha^{(e)}. \tag{40}$$

Consider now the 2^n states of the counter. It is clear from (40) that in the successors of these states Q_0 takes the value 1 exactly 2^{n-2} times if $k = 1$ and $3 \cdot 2^{n-2}$ times if $k = 0$. In an injective counter, Q_0 should take the value 1 exactly 2^{n-1} times.

(ii) The cascade formed by the strings B and A is not empty. In that case, we denote by $\mathbf{q}_1$ the state of that cascade without its last flip-flop, the state of which is q_r, and by $\mathbf{q}_1'$ and q_t the state of the string C and of the right-hand F flip-flop, respectively. Note that if the string A is empty, the flip-flop q_r belongs to the string B: this does not affect the validity of the following proof. It now becomes clear that the states

$$(\alpha, q_0, \mathbf{q}_1, q_r, \mathbf{q}_1', q_t) = (\alpha, x, \mathbf{x}, x \oplus \bar{e} \oplus \alpha, \mathbf{x}, \bar{h}) \qquad (x \in \{0, 1\})$$

have identical successors. Indeed the state

$$Q_0 = x^{(\bar{e})} \alpha^{(e)} \oplus x^{(e)} (x^{(e)} \oplus \alpha^{(\bar{e})}) = \alpha^{(e)}$$

is independent of x. Q.E.D.

Thanks to Theorem 9 and Lemma 9 it is clear that, in an injective simple counter, a basic three-pole should fulfill one of the two following conditions.

Condition 1. The three-pole controls the two inputs of a second three-pole.

Condition 2. The three-pole controls one of the inputs of two three-poles. These conditions, illustrated by Fig. 15, will now be briefly discussed.

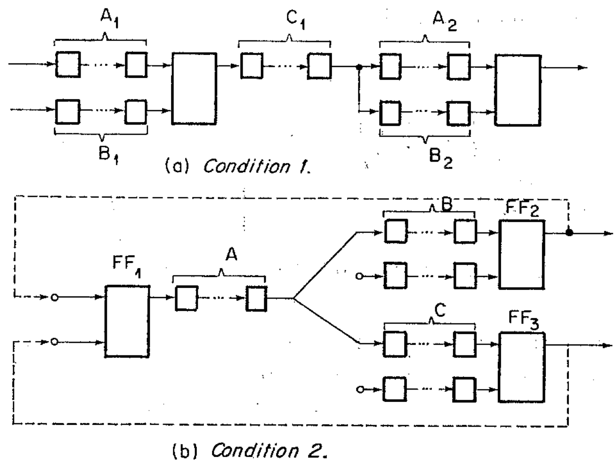

FIG. 15. The two possible conditions for a basic three-pole in an injective simple counter.

If Condition 1 is realized for all three-poles in the simple counter, the latter presents itself as a kind of "loop" and it will be called a *generalized loop-counter*. It is clear that in a generalized loop-counter the input strings A_i, B_i do not contain any $D^{(e)}$ flip-flop (Lemma 8) and that all the $D^{(e)}$ flip-flops eventually present in the output strings C_i may be regrouped in a single output string (Theorem 3). We may thus restrict our investigations to generalized loop-counters made up of:

(a) a string of $D^{(e)}$ flip-flops,

(b) basic three-poles containing only $T^{(e)}$ flip-flops in the input and output strings.

The structure of generalized loop-counters is illustrated by Fig. 16. These counters are the fundamental injective simple nonlinear counters (see Theorem 11). They are more precisely characterized by the following theorem.

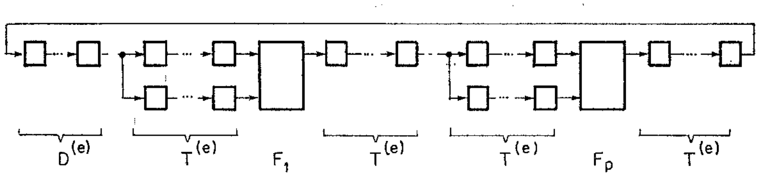

FIG. 16. Structure of the generalized loop-counter.

THEOREM 10. *A generalized loop-counter is injective iff its $D^{(e)}$ string is not empty.*

Proof. If the $D^{(e)}$ string is empty, two complementary states such that $\forall i$ $F_{i0} = F_{i1}$ have the same successor. If the $D^{(e)}$ string is not empty, it is easily shown that two distinct states always yield distinct successors; the reasoning is similar to that of Theorem 6, but applies to equations of the types (12)–(17). Q.E.D.

COROLLARY. *A generalized loop-counter containing p F flip-flops contains at least $(2p + 1)$ flip-flops.*

We now turn to the discussion of Condition 2, illustrated by Fig. 15b. It is first clear that, to escape the situation forbidden by Lemma 8, the two controlled flip-flops $FF2$ and $FF3$ have to react directly (i.e., without interposed linear flip-flops) and with suitable polarities on the inputs F_{10} and F_{11} of $FF1$. It turns out that $FF2$ and $FF3$ also fall under Condition 2, and this implies the emptiness of the strings A, B, and C. Thus, if in a simple injective counter a single flip-flop realizes Condition 2, there are no linear flip-flops and all the F flip-flops in the counter satisfy the same condition. The general structure of these counters, called hereafter *pathological counters*, is illustrated in Fig. 17. The name pathological counter is explained by the following theorem.

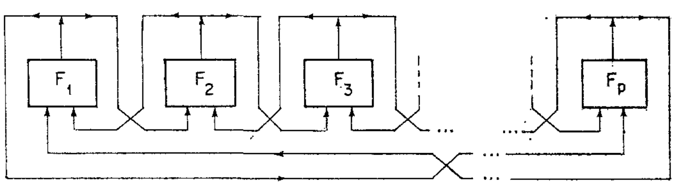

FIG. 17. Structure of the pathological counters.

THEOREM 11. *Except for $n = 3$, no pathological counter is injective.*

Proof. We consider (Fig. 18) two neighbor flip-flops in a pathological counter. Clearly, we may assume that the input of FF_0 controlled by $FF1$ is the K_0 input (reduction to that situation is always possible by complementation

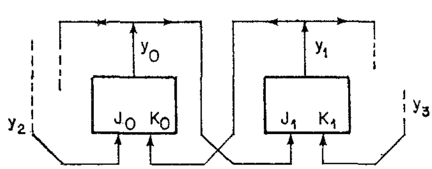

FIG. 18. Illustration of Theorem 11.

of y_0) and furthermore that $K_0 = y_1$ (if $K_0 = \bar{y}_1$, the complementation of y_2 leads back to the former case). The input equation for FF_0 is thus

$$Y_0 = \bar{y}_0 y_2 \vee y_0 \bar{y}_1 .$$

In that situation, there are four possibilities with regard to FF_1, namely, $y_0 \in \{J_1, \bar{J}_1, K_1, \bar{K}_1\}$. In these four situations, the excitation equations for FF_1 are

$$\begin{aligned}
&1.\ Y_1 = \bar{y}_1 y_0 \vee y_1 \bar{y}_3 ,\\
&2.\ Y_1 = \bar{y}_1 \bar{y}_0 \vee y_1 \bar{y}_3 ,\\
&3.\ Y_1 = \bar{y}_1 y_3 \vee y_1 \bar{y}_0 ,\\
&4.\ Y_1 = \bar{y}_1 y_3 \vee y_1 y_0 ;
\end{aligned}$$

note that the polarity of y_2 and y_3 is irrelevant in the present proof. We now compute in these four situations the products $Y_1 Y_0$. It is clear that, if the counter is injective, these products should have a weight of 2^{n-2} (i.e., assume the value 1 on exactly 2^{n-2} vertices of the n-cube). One obtains

$$\begin{aligned}
&1.\ Y_1 Y_0 = \bar{y}_3 y_2 y_1 \bar{y}_0 \vee \bar{y}_1 y_0 ; \qquad (5 \cdot 2^{n-4}),\\
&2.\ Y_1 Y_0 = y_2 \bar{y}_1 \bar{y}_0 \vee \bar{y}_3 y_2 y_1 \bar{y}_0 ; \qquad (3 \cdot 2^{n-4}),\\
&3.\ Y_1 Y_0 = y_3 y_2 \bar{y}_1 \bar{y}_0 \vee y_2 y_1 \bar{y}_0 \vee y_3 \bar{y}_1 y_0 ; \qquad (5 \cdot 2^{n-4}),\\
&4.\ Y_1 Y_0 = y_3 y_2 \bar{y}_1 \bar{y}_0 \vee y_3 \bar{y}_1 y_0 ; \qquad (3 \cdot 2^{n-4}),
\end{aligned}$$

respectively. The associated weights are indicated under the hypothesis $y_2 \neq y_3 \neq \bar{y}_2$ which, by definition of a pathological counter, corresponds to $n > 3$. Since none of these weights is equal to 2^{n-2}, no pathological counter is injective.

Q.E.D.

When $y_2 = y_3$, the solutions $y_0 = J_1$ and $y_0 = \bar{K}_1$ are acceptable (with respect to the above weight argument), while, if $y_2 = \bar{y}_3$, one retains $y_0 = \bar{J}_1$ and $y_0 = K_1$. The same reasoning may be extended to the pairs of flip-flops $\{FF_0, FF_2\}$ and $\{FF_1, FF_2\}$. This process finally yields three nonequivalent injective pathological counters. These three counters are displayed in Fig. 19 together with their state graphs.

7. Applications

Circular Counters

The foregoing section shows that any circular counter containing at least three flip-flops should belong to the class of generalized loop-counters. Indeed, it cannot be linear nor pathological. The purpose of the present section is to present arguments that allow one to distinguish circular counters from noncircular injective ones. This will bring down the number of candidate circular counters. The resulting computation will strengthen the conjecture that no circular counter exists for $n \geqslant 4$.

We thus refer to Fig. 16, which displays the structure of generalized loop-counters, and first state two additional properties of circular counters.

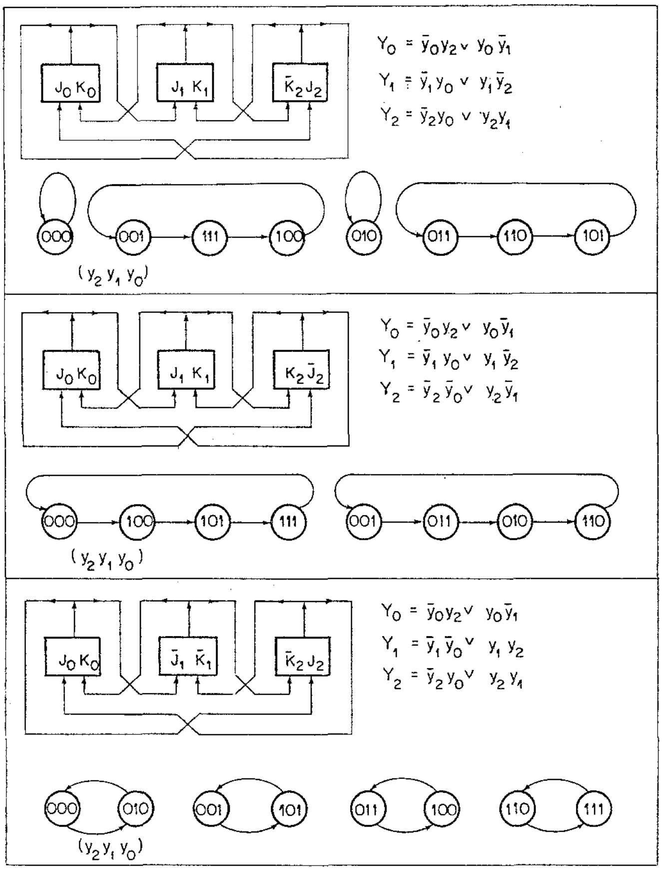

FIG. 19. The three injective pathological counters.

LEMMA 10. *In a circular counter:*

(i) *The output strings of the F flip-flops are empty.*

(ii) *The input strings controlling the J and K inputs to a given F flip-flop are a $T^{(e)}$ and a $T^{(\bar{e})}$ sequence.*

Proof. (i) Consider the subcounter displayed in Fig. 20 and note that for any q_0, there is a state $\mathbf{q}$ and an input letter x such that the following are all stable:

(a) the flip-flops in the output string A,

(b) the flip-flops in the F_{q_0} input string,

(c) the F flip-flop.

Furthermore, if the string A is not empty, the stabilizing value of x only depends on the polarity of the first $T^{(e)}$ flip-flop in the A string and is thus independent of q_0. It is thus always possible to stabilize a loop in the counter of Fig. 16.

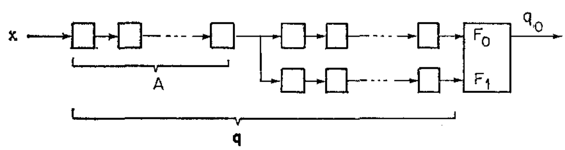

FIG. 20. A subcounter.

(ii) The same argument applies since, if both input sequences have the same polarity, the input stabilizing value is again independent of q_0. Q.E.D.

The candidate circular counters are thus made up of a $D^{(e)}$ sequence and of cells belonging to one of the following two types:

(a) The $\mathscr{T}$ *cell* where the J input string is a T sequence and where the K input string is a $\bar{T}$ sequence.

(b) The $\bar{\mathscr{T}}$ *cell* where the J input string is a $\bar{T}$ sequence and where the K input string is a T sequence.

Note that if one input string is empty, the corresponding input should be given the appropriate polarity. This is illustrated by Fig. 21, which displays the three types of $\mathscr{T}$-cells. Finally, consider the cascade of a $\mathscr{T}^{(e)}$ and of a $\mathscr{T}^{(h)}$ cell.

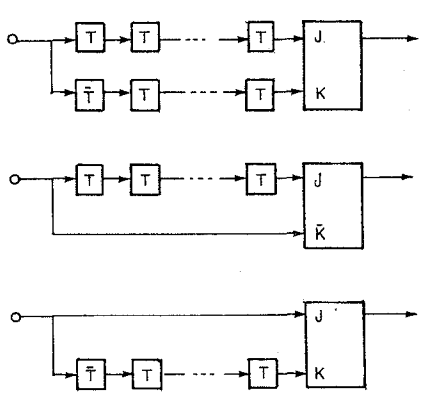

FIG. 21. The three types of $\mathscr{T}$-cells.

Apply to the first F flip-flop the isomorphism of Theorem 1: the cascade is replaced by a $\mathscr{T}^{(\bar{e})}\mathscr{T}^{(\bar{h})}$ cascade. There are thus only two types of candidate circular counters: we may characterize these counters by the sequences

$$\bar{D}\mathscr{T}\mathscr{T}\mathscr{T}\cdots\mathscr{T} \tag{41}$$

and

$$D\mathscr{T}\mathscr{T}\mathscr{T}\cdots\mathscr{T},$$

where $\bar{D}$ and D stand for $\bar{D}$ and D sequences. The counters of the second type, however, are again eliminated by a loop stabilization argument so that we may normalize the investigated structures to type (41).

The counters to be investigated are thus completely described by a vector having $(2p + 1)$ integer components,

$$[d; j_1, k_1; j_2, k_2; \cdots; j_p, k_p],$$

where d is the number of flip-flops in the D string and where j_i (resp. k_i) is the number of T flip-flops in the J_i (resp. K_i) input string to the flip-flop F_i. This vector is called the *structure vector* of the counter.

The number of structure vectors to be enumerated is furthermore reduced by the observation that the vectors

$$[d; j_1, k_1; j_2, k_2; \cdots; j_p, k_p]$$

and

$$[d; j_p, k_p; j_1, k_1; \cdots; j_{p-1}, k_{p-1}]$$

describe isomorphic counters.

Analysis results have been obtained by means of a computer program for $3 \leqslant n \leqslant 9$. For $n = 3$, one obtains the circular counter displayed in Fig. 22 together with its state graph. This counter has been described by Manning (1972). No other circular counter has been found up to $n = 9$. This strongly supports the conjecture that no circular counter exists for $n > 3$. However, no proof of this fact has been obtained. Table II presents the cycle structure for $3 \leqslant n \leqslant 7$.

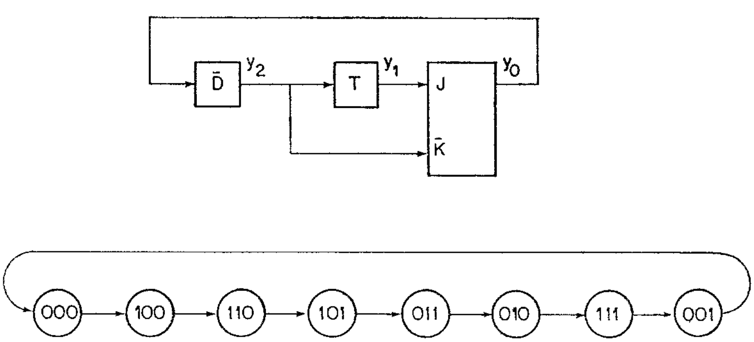

FIG. 22. The [1; 1, 0] circular counter.

TABLE II — Cycle Structure of Some Generalized Loop-Counters

n	p	d	j_1	k_1	j_2	k_2	j_3	k_3	Cycle lengths					
3	1	1	0	1					8					
4	1	1	0	2					6	10				
	1	1	1	1					8	8				
	1	2	0	1					7	9				
5	1	1	0	3					14	18				
	1	1	1	2					6	6	8	12		
	1	2	0	2					5	27				
	1	2	1	1					8	24				
	1	3	0	1					3	29				
	2	1	0	1	0	1			6	26				
6	1	1	0	4					30	34				
	1	1	1	3					10	54				
	1	1	2	2					4	4	8	16	16	16
	1	2	0	3					5	59				
	1	2	1	2					24	40				
	1	3	0	2					3	16	17	28		
	1	3	1	1					4	60				
	1	4	0	1					11	53				
	2	1	0	1	0	2			12	52				
	2	1	0	1	1	1			6	6	22	30		
	2	1	0	1	2	0			31	33				
	2	2	0	1	0	1			3	6	22	33		
7	1	1	0	5					8	8	10	102		
	1	1	1	4					6	6	12	104		
	1	1	2	3					20	24	24	60		
	1	2	0	4					36	92				
	1	2	1	3					16	24	26	62		
	1	2	2	2					16	16	48	48		
	1	3	0	3					8	9	15	16	40	40
	1	3	1	2					36	92				
	1	4	0	2					38	90				
	1	4	1	1					4	12	28	84		
	1	5	0	1					13	115				
	2	1	0	1	0	3			8	120				
	2	1	0	1	1	2			6	8	14	18	26	56
	2	1	0	1	2	1			48	80				
	2	1	0	1	3	0			61	67				
	2	1	0	2	0	2			14	19	34	61		
	2	1	0	2	1	1			12	22	28	66		
	2	1	1	1	1	1			4	4	60	60		
	2	2	0	1	0	2			3	27	48	50		
	2	2	0	1	1	1			32	96				
	2	2	0	1	2	0			3	125				
	2	3	0	1	0	1			31	97				
	3	1	0	1	0	1	0	1	3	5	15	16	41	48
	3	1	0	1	1	0	0	1	11	23	29	65		

8. Conclusions

As the Introduction stated, the main goal of this study was the establishment of a tight relationship between a structural property (essentially the generalized loop structure) and a behavioral property (the injective character).

So far, it seems that the interest of the counters that have been studied is more theoretical than practical. For example, it is possible to count in binary by means of *JK* flip-flops and only one additional two-input AND gate per flip-flop. For small values of n, these AND gates are not even required if an adequate use is made of available multiple-input *JK* flip-flops. However, our knowledge about counters composed only of *JK* flip-flops is not complete enough to draw final conclusions.

Among the problems left open by this study, are:

(i) the realization of cycles of arbitrarily prescribed length with a minimum number of flip-flops,

(ii) synthesis methods for counters whose transition graph is connected,

(iii) synthesis methods for reliable counters.

With respect to point (i), it is very easy to exhibit an existence proof since the shift register trivially produces cycles of length n. The counters obtained in this way are obviously far from being minimal. Finally, from experimental results, we conjecture that generalized loop-counters have an even number of cycles for $n \geqslant 4$.

Acknowledgments

The authors are indebted to their colleagues J. P. Deschamps, J. M. Goethals, and J. J. Quisquater for fruitful discussions. Thanks are also due to an anonymous referee for helpful comments and suggestions.

Received: January 16, 1976; revised: May 20, 1976

References

Denes, J. (1968), On transformations, transformation-semigroups and graph, *in* "Theory of Graphs," Proceedings of the Colloquium held at Tihany, Hungary (September 1966), Academic Press, New York.

Dietmeyer, D. L. (1971), "Logic Design of Digital Systems," Allyn and Bacon, Boston, Mass.

Elspas, B. (1959), The theory of autonomous linear sequential networks, *IRE Trans. Circuit Theory* **CT6**, 45–60.

Ginzburg, A. (1968), "Algebraic Theory of Automata," Academic Press, New York.

Manning, F. (1972), "Autonomous, Synchronous Counters Constructed only of *J-K* Flip-Flops," MAC TR-96, M.I.T., Cambridge, Mass.

Manning, F. and Fenichel, R. (1976), Synchronous counters constructed entirely of *J-K* flip-flops, *IEEE Trans. Computers* **C-25**, 300–306.

Peterson, W. W. (1961), "Error Correcting Codes," M.I.T. Press, Cambridge, Mass.

Phister, M. (1958), "Logical Design of Digital Computer," Wiley, New York.

Pless, V. (1976), Mathematical foundation of interconnected *JK* flip-flops, *Inform. Contr.* **30**, 128–142.

Rudeanu, S. (1974), "Boolean Functions and Equations" North–Holland, Amsterdam.