ESTUDIO FORMAL DE REDES LINEALES Y SU APLICACIÓN A LA SÍNTESIS DE CONTADORES

T. OSES, J. AGUILÓ, LL. HUGUET

A partir de la identificación de la función estado siguiente de las máquinas sequenciales lineales con el conjunto de funciones de $GL_n(Z_2)$ y $A_n(Z_2)$ es posible tratar formalmente los problemas de codificación de estados internos para el caso de síntesis con elementos biestables J-K pudiendo establecer una generalización al caso de la síntesis con biestables z-Fivex.

Los resultados teóricos obtenidos se aplican a la síntesis de contadores, utilizando módulos base para su implementación, lo cual supone una optimización tanto desde el punto de vista de diseño como de superficie ocupada. También se establece una comparación entre las dos estructuras estudiadas.

1. INTRODUCCION.

Los problemas correspondientes a la asignación de estados en m.s. sincronas han sido abordadas desde distintos puntos de vista y por diversos autores /1/, /2/ y /3/. En todos los casos se persigue una cierta optimización de las m.s. a través de la asignación, ya sea coste, velocidad de respuesta, etc. o bien superficie de silicio ocupada, nº de conexiones topologia. En ninguno de los casos se ha podido dar una solución analítica general al problema mientras que, por otra parte, las soluciones heurísticas alcanzadas hasta el momento tropiezan con las grandes dificultades habituales en la resolución de un problema NP-completo, tiempo de cálculo exponencial y crecimiento también exponencial de los recursos de memoria utilizados.

La formalización matemática del problema para conseguir unas posibilidades de tratamiento independientes del problema en sí, es quien ha conseguido hasta la fecha los mejores resultados experimentales /4/, /5/ y /6/, consiguiendo además fácilmente un segundo objetivo, delimitar conjuntos de m.s. con el mismo óptimo independiente del criterio de optimización elegido.

En el presente trabajo se abordan formalmente los problemas de codificación de estados internos en el caso de síntesis con elementos biestables JK englobando a trabajos anteriores con biestables D y entreviendo claramente la posibilidad de generalización a los elementos de la familia z-FIVEX.

A partir de estos resultados es posible encontrar de manera sistemática la síntesis de cualquier máquina secuencial autónoma (m.s.a.) llegando a obtener unos módulos base para su implementación en forma de circuito integrado. Desde este punto de vista, se hace la comparación entre los dos tipos de implementación estudiado.

2. FORMALIZACION MATEMATICA

Definimos una máquina secuencial lineal como aquella máquina cuyas funciones de salida y de estado siguiente son funciones lineales.- En el caso particular en que el circuito combinacional de salida sea nulo la m.s. será lineal si lo es la función, f, de estado siguiente,

- T. Oses, J. Aguiló, LL. Huguet - Departament d'Informàtica de la Universitat Autònoma de Barcelona.- Bellaterra (Barcelona)
- Article rebut el Abril del 1982.

En general la función f correspondiente al endomorfismo de $B^n \to B^n$ es de la forma

$$f = (f_1, f_2, \ldots, f_n) : B^n \to B^n \quad y \quad f_i : B^n \to B$$

así para todo $(v_1, v_2, \ldots, v_n) \in B^n$; $B = \{0,1\}$

$$f(v_1, v_2, \ldots, v_n) = (v_1', \ldots, v_n') = (f_1(v_1 \ldots \ldots v_n), \ldots f_n(v_1, \ldots, v_n))$$

En el caso en que f sea una aplicación biyectiva $f \in GL_n(Z_2)$ es decir, al grupo lineal de dimensión n sobre Z_2 y por tanto admite una representación matricial F cuyos elementos $f_{ij} \in Z_2$ $\forall i, j$ y tal que $\det(F) = 1$.

La matriz F aplicada a un elemento $x = (x \ldots \ldots, x_n) \in B^n$ opera de la siguiente forma:

$$F(x) = ((f_{11} \cdot x_1 \oplus f_{12} \cdot x_2 \oplus \ldots f_{1n} \cdot x_n), \ldots \ldots (f_{n1} \cdot x_1 \oplus \ldots \oplus f_{nn} \cdot x_n)) = (y_1, \ldots, y_n) = y$$

Podemos observar que las filas de la matriz F se corresponden con las componentes f_i de la función lineal f. La función f representa también un grafo dirigido $G = (V,E)$ donde $V = \{B^n\}$ y

$$E = \{(v_i, v_j) \in V \times V \mid v_j = f(v_i)\}$$

En teoría de la conmutación, también se considera función lineal aquella en la forma

$$f_i = c_0 +_2 \sum c_{ij} x_j \quad \text{con } c_0 \in \{0,1\}$$

Si una función $\underline{f} = (f_1, \ldots, f_n)$ tiene alguna de sus componentes con $c_0 = 1$ y las f_i son linealmente independientes, la función $\underline{f}$ puede representarse por una matriz $A \in A_n(Z_2)$ siendo éste el grupo de las finidades sobre Z_2. Dichas afinidades pueden obtenerse a partir del grupo lineal $GL_n(Z_2)$ sin más que sumar una traslación.

$$A_n(Z\ ) = GL_n(Z\ ) + X, \quad \forall X \in B^n$$

3. PROPIEDADES DE $GL_n(Z_2)$.

Una vez establecida la relación entre las máquinas secuenciales lineales y el conjunto de matrices pertenecientes a $GL_n(Z_2)$ podemos definir la siguiente familia de subconjuntos, L_i, de $GL_n(Z_2)$

$$L_1 = \{A \in GL_n(Z_2) \mid \quad \forall i \quad \sum_j a_{ij} = 1\}$$

$$L_z = \{A \in GL_n(Z_2) \mid \quad \forall i \quad \sum_j a_{ij} \leqslant a_{ii} + (z-1)\}, \forall z > 1$$

evidentemente $L_1 \subset L_2 \subset L_3 \subset \ldots \subset L_n = GL_n(Z_2)$

Definimos la relación de conjugación, $\underset{2}{\simeq}$, entre elementos de $GL_n(Z_2)$ en la forma siguiente.

Dadas A y $B \in GL_n(Z_2)$

$$A \simeq B \Longleftrightarrow \exists U \in GL_n(Z_2) \mid U^{-1} A U = B$$

La relación anterior, evidentemente, es de equivalencia.

Teorema 1.- Sea $F \in GL_n(Z_2)$ con $P_F(x)$ su polinomio característico irreducible o producto de irreducibles distintos y $Q_F(x)$ su polinomio anulador, resulta que

$$P_F(x) = P_{F'}(x) \text{ y } Q_F(x) = Q_{F'}(x) \Leftrightarrow F \underset{2}{\simeq} F'$$

Demostración:

Si F y F' tienen sus polinomios característico y anulador iguales admiten una misma forma diagonal F_D, es decir

$$\exists U_1 \in GL_n(Z_2) \mid U_1^{-1} F U_1 = F_D \quad y$$

$$\exists U_2 \in GL_n(Z_2) \; U_2^{-1} F' U_2 = F_D$$

Por tanto

$$U_1^{-1} F U_1 = U_2^{-1} F' U_2 \Rightarrow U_2 U_1^{-1} F U_1 U_2^{-1} = F'$$

$$F' = (U_1 U_2^{-1})^{-1} F (U_1 U_2^{-1}) = U_3^{-1} F U_3 \Longrightarrow F' \underset{2}{\simeq} F$$

En sentido contrario también se verifica ya que un cambio de base no modifica ni el polinomio característico ni el anulador.

Si el polinomio $P_F(x)$ lo expresamos en la forma $x^n +_2 \ldots +_2 c_1 x +_2 c_0$ la matriz F' isomorfa a F, $F' \underset{2}{\simeq} F$, puede encontrarse en la forma,

$$\begin{pmatrix} c_{n-1} & 1 & 0 & \ldots & 0 \\ c_{n-2} & 0 & 1 & \ldots & 0 \\ \cdot & \cdot & \cdot & \ldots & \cdot \\ c_1 & 0 & 0 & \ldots & 1 \\ c_0 & 0 & 0 & \ldots & 0 \end{pmatrix} = F' \qquad (1)$$

Esto también se cumple en el caso particular en que $P_F(x)$ sea un polinomio irreducible o potencia de polinomio irreducible.

Corolario 1.- Si $P_F(x) \neq Q_F(x)$ y sean

$$P_F(x) = p_1^{\alpha_1}(x) \cdot p_2^{\alpha_2}(x) \ldots\ldots\ldots p_k^{\alpha k}(x) \quad \text{y}$$

$$Q_F(x) = p_1^{\beta_1}(x) \cdot p_1^{\beta_1}(x) \ldots\ldots\ldots p_k^{\beta k}(x) \quad \text{con}$$

$$\alpha_i \geqslant \beta_i \geqslant 1 \quad \forall i$$

su descomposición en polinomios primos. Podemos obtener $F' \underset{2}{\simeq} F$ tal que

$$F' = \begin{pmatrix} [p_1^{\beta_1}(x)] & 0 & & & & & \\ & [p_1^{\gamma_{11}}(x)] & 0 & & & & \\ & & \ddots\ [p_1^{\gamma_{1r}}(x)] & 0 & & & \\ & & & [p_2^{\beta_2}(x)] & 0 & & \\ & & & & [p_2^{\gamma_{21}}(x)] & 0 & \\ & & & & & \ddots\ [p_2^{\gamma_{2s}}(x)] & \\ & & & & & & \ddots \end{pmatrix} \qquad (2)$$

con $\sum_r \gamma_{ir} = \alpha_i - \beta_i$.

Donde $[p_j(x)]$ representa una matriz cualquiera cuyo polinomio característico $p_j(x)$ es irreducible, coincidiendo por tanto con su anulador. Por otra parte $[p_j^{\beta_j}(x)]$ representa una matriz cuyo polinomio característico coincide con el anulador siendo este una potencia de polinomio irreducible.

La matriz (2) puede expresarse también como

$$F' = [p_1^{\beta_1}(x)] \oplus [p_1^{\gamma_{11}}(x)] \oplus\ldots\oplus [p_1^{\gamma_{1r}}(x)] \oplus\ldots$$
$$\ldots\oplus [p_k^{\beta_k}(x)] \oplus [p_k^{\gamma_k}(x)] \oplus\ldots\oplus [p_k^{\gamma_{ks}}(x)]$$

donde el operador $\oplus$ indica suma directa de matrices. Los coeficientes γ_{ir} se obtienen a partir de las dimensiones de los núcleos de los subespacios vectoriales en que puede descomponerse el espacio vectorial total /7/.

Teniendo en cuenta la relación de isomorfía de grafos, las funciones

$$F: B^n \longrightarrow B^n$$
$$x \longrightarrow y = F(x) \qquad \text{y}$$

$$F^{-1}: B^n \longrightarrow B^n$$
$$y = F(x) \longrightarrow F^{-1}(y) = x$$

representan grafos isomorfos ya que la matriz $A \in GL_n(Z_2)$ asociada a la función F tiene determinante igual a 1, por tanto F biyectiva.

Invertir la función equivale a cambiar el sentido de los arcos entre el nodo x y F(x), por consiguiente podemos afirmar que A y A^{-1} representan grafos isomorfos a pesar de que, en general, sus polinomios característicos son distintos.

Ejemplo

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \qquad P_A(\lambda) = \lambda^4 \oplus \lambda \oplus 1;\ \{C_A\} \longrightarrow 1^1 \quad 15^1$$

$$A^{-1} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad P_{A^{-1}}(\lambda) = \lambda^4 \oplus \lambda^3 \oplus 1;\ \{C_{A^{-1}}\} \longrightarrow 1^1 \quad 15^1$$

En este caso vemos que los polinomios correspondientes a A y A^{-1} son distintos pero sin embargo $F_A \simeq F_{A^{-1}}$ según la relación de isomorfía de grafos. Esto permite enunciar el siguiente

Teorema 2.- Si $P(\lambda)$ es irreducible, ($P(\lambda) = Q(\lambda)$), y $P'(\lambda)$ es su conjugado, las clases de equivalencia correspondientes a $P(\lambda)$ y $P'(\lambda)$ son isomorfas.

Demostración:

$$P'(\lambda) = \lambda^n \, (P(\lambda^{-1}))$$

y $P'(\lambda)$ no es más que el polinomio característico asociado a la matriz inversa y $P'(\lambda)$ es irreducible.

4. CLASIFICACION DE $GL_n(Z_2)$

Según el teorema 1 la relación de equivalencia-2 conserva el polinomio característico y su descomposición en polinomios elementales, por consiguiente, para un n dado las clases de isomorfía, como máximo, son las correspondientes a

1) Polinomios irreducibles de grado n para los cuales el polinomio característico y anulador coinciden.

2) Polinomios de grado n potencia de polinomio irreducible con polinomio característico y anulador iguales.

3) Composición de casos anteriores cuyo polinomio característico podrá expresarse como producto de polinomios irreducibles elevados a diferentes potencias.

En este tercer caso $P_n(\lambda)$ podremos expresarlo en la forma

$$P_n(\lambda) = (P_{r_1}(\lambda))^{s_1} (P_{r_2}(\lambda))^{s_2} \ldots$$

con la condición $\sum_i r_i s_i = n$.

Ahora bien, el polinomio anulador $Q_n(\lambda)$ puede ser distinto de $P_n(\lambda)$ luego dentro del apartado 2) podremos considerar

2.1) $P_n(\lambda) = Q_n(\lambda)$ esto corresponde a una clase de equivalencia en la cual existirá un elemento J_1 de la forma

$$J_1 = \left(\begin{array}{ccc|ccc} P_{r_1}(\lambda) & 1 & & & & \\ & \ddots & 1 & & & \\ & s_1 & P_{r_1}(\lambda) & & & \\ \hline & & & P_{r_i}(\lambda) & 1 & \\ & & & & \ddots & 1 \\ & & & & s_i & P_{r_i}(\lambda) \end{array}\right)$$

según la diagonalización de Jacobson.

2.2) Si $P_n(\lambda) \neq Q_n(\lambda)$ éste corresponde a una composición y la clase de equivalencia tendrá un representante J_2 de la forma

$$J_2 = \begin{pmatrix} B_{r_1} & & & \\ & B_{r_2} & & \\ & & \ddots & \\ & & & B_{r_i} \end{pmatrix}$$

donde cada una de las cajas B_{r_i} corresponde a la forma canónica de Jacobson del polinomio irreducible $(p_i(\lambda))$, obteniendo como resultado una matriz análoga a la (2).

5.1 - MATRICES

Lema 1. $A \in L_2 \mid P_n(\lambda)$ es irreducible $\Longrightarrow$ la matriz A' con $a'_{ij} = a_{ij} \oplus \delta_{ij}\, a_{ij}$ es tal -- que A' $\in S_n$.

Demostración:

A' tiene un elemento distinto de cero por fila ya que en caso contrario A' tendrá una fila de ceros. Sea i esta fila, el $\det(A \oplus \lambda I)$ puede desarrollarse por la fila i y

$$\det(A \oplus \lambda I) = (a_{ii} \oplus \lambda) \det \Delta_{ii}$$

luego $P(\lambda)$ no es irreducible contra la hipótesis.

En la misma forma A' tiene un elemento dis-- tinto de cero por columna ya que en caso contrario A' tendría una columna de ceros y podría desarrollarse por la columna i obteniendo que

$$\det(A \oplus \lambda I) = (a_{ii} \oplus \lambda) \det \Delta_{ii}$$

Lema 2. $A \in S_n \Longrightarrow$ A admite una descomposi-- ción en r cajas en la forma

$a_{i(i+1)} = 1 \qquad i \neq m_1, m_2, \ldots, m_r$

$a_{m_j 1} = 1 \qquad j = 1, 2, \ldots, r$

$$\begin{pmatrix} \begin{matrix} 0 & 1 & & \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \\ 1 & 0 & \cdots & 0 \end{matrix} & & \\ & \ddots & \\ & & \begin{matrix} 0 & 1 & & \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \\ 1 & 0 & \cdots & 0 \end{matrix} \end{pmatrix}$$

Demostración:

Evidente si se toma la matriz A de incidencia de un grafo.

Teorema 3. $A \in L_2 \Longrightarrow P_n(\lambda) = \prod_i P_i(\lambda) \quad (3)$

donde $P_i(\lambda)$ son todos de la forma $P_i(\lambda) = (c_{jj} \ldots c_{kk} \oplus 1)$ con $c_{jj} = a_{jj} \oplus \lambda$

Demostración:

Si la matriz A' cuyos elementos $a'_{ij} = a_{ij}\bar{\delta}_{ij}$ es tal que $A' \in S_n$ por aplicación del Lema 2 obtendremos la descomposición de A' en r cajas a través de una permutación de filas y columnas. Aplicando esta misma -- permutación a la matriz A obtenemos la descomposición buscada.

Si $A' \notin S_n$ por el Lema 1 $P_n(\lambda)$ no es irreducible y por tanto A puede obtenerse por composición y $P_n(\lambda) = (\lambda \oplus 1)\, P_{n-1}(\lambda)$ quedando la matriz de la forma

$$A \simeq \begin{pmatrix} 1 & c_i \\ & A_1 \end{pmatrix} \quad \text{con } P_{A_1}(\lambda) = P_{n-1}(\lambda)$$
$$\text{y } c_i \in \{0,1\}$$

A la matriz A_1 podemos aplicarle las consi-- deraciones anteriores hasta obtener una A_i tal que $A'_i \in S_n$.

Una vez obtenida la expresión de $P_n(\lambda)$ en la forma dada por la ecuación (3) la descomposición en polinomios elementales nos determinará que elementos c_i deben ser igual a uno según hemos visto en los apartados 4.3.1 y --- 4.3.2.

Corolario 2.- Una matriz cualquiera $A \in L_2$ - puede transformarse mediante un cambio de base en suma directa de matrices de la forma:

$$\begin{bmatrix} a_{11} & 1 & 0 & \cdots & 0 \\ 0 & a_{22} & 1 & \cdots & 0 \\ \vdots & & & \ddots & \\ a_{n1} & 0 & 0 & \cdots & a_{nn} \end{bmatrix}$$

donde $a_{jj}, a_{n1} \in \{0,1\}$ y

$$\prod_j a_{jj} \oplus a_{n1} = 1$$

Denominamos T-matrices, a las matrices de la forma anterior.

Podemos concluir, pues, que cualquier m.s. - puede ser representada, salvo isomorfías, -- por una T-matriz ó composición de T-matrices.

6. PROPIEDADES DE LAS T-MATRICES.

En el apartado anterior hemos visto que to-- das las clases de conjugación de L_2 contie-- nen al menos un elemento que corresponde a - una T-matriz o composición de T-matrices.

Lema 3.- Dadas dos matrices A y B∈{T-matri-- ces} y tales que

$$\left.\begin{array}{l} a_{ij} = b_{ij} \quad \forall i \neq j \\ \sum\limits_i a_{ii} = \sum\limits_i b_{ii} \end{array}\right\} \longrightarrow A \underset{2}{\simeq} B$$

Observemos que un cambio de base en la forma

$$U = \begin{array}{c} \left(\begin{array}{c|cc|c} I & & & \\ \hline & 1 & 0 & \\ & 1 & 1 & \\ \hline & & & I \end{array}\right) \begin{array}{l} \\ \leftarrow i-1 \\ \leftarrow i \\ \\ \end{array} \\ \begin{array}{cc} \uparrow & \uparrow \\ i-1 & i \end{array} \end{array}$$

permuta los elementos i e $i-1$ siempre y - cuando estos elementos sean distintos /8/.

La aplicación del Lema 3 nos permite afirmar que las T-matrices están caracterizadas por el número de elementos de la diagonal distin tos de cero pero no por las posiciones ocupa das.

Teorema 4.-

Sea $\Gamma_2 = \{A \in GL_n(Z_2) \quad A = U^{-1} L_2 U\}$

$$A \in \Gamma_2 \longleftrightarrow P_n(\lambda) = \prod_j (\lambda^{s_j} (\lambda \oplus 1)^{t_j} \oplus 1)^{r_j}$$

donde $s_j, t_j, r_j \in N$ y $\sum\limits_j (s_j+t_j) r_j = n$

Demostración:

Según el Teorema 3 y el Lema 3 cada una de - las cajas en que puede descomponerse A tiene como polinomio característico

$$P_n(\lambda) = \lambda^{s_j}(\lambda \oplus 1)^{t_j} \oplus 1$$

$$P_n(\lambda) = \lambda^{s_j} (\lambda \oplus 1)^{t_j} \oplus 1 \qquad (4)$$

donde s_j = nº de ceros sobre la diagonal y - t_j = nº de unos sobre la diagonal.

Si de la descomposición resultan r_j cajas -- iguales el polinomio característico será en- tonces de la forma propuesta. En particular si $P_n(\lambda)$ es irreducible $r = 1$; $r_j = 0$

$\forall j > 1.$

Hasta n=4 las T-matrices cubren todo el ---- $GL_4(Z_2)$ pues aunque existe un polinomio irre ducible $P(\lambda) = \lambda^4 \oplus \lambda \oplus 1$ que no es posible expresarlo según la ecuación (2) este corres ponde al polinomio conjugado del $\lambda^4 \oplus \lambda^3 \oplus 1$ el cual admite descomposición en dicha forma.

Para n=6 el polinomio irreducible

$$\lambda^6 \oplus \lambda^4 \oplus \lambda^2 \oplus \lambda \oplus 1 \qquad (5)$$

no admite descomposición según la ecuación - (2) y su conjugado tampoco la admite.

Se puede comprobar que la clase de isomorfía correspondiente al polinomio (5) no aparece para las T-matrices. Esto nos permite asegu- rar la falsedad de la conjetura Fabregat-Agui ló (8) y establecer el siguiente

Corolario 4.-

$$U^{-1} L_2 U \neq GL_n(Z_2)$$

No es posible obtener $GL_n(Z_2)$ a través de cam bios de base en los elementos del conjunto -- $L_2 \subset GL_n(Z_2)$.

Esto significa que las clases de isomorfía - obtenidas a través del grupo lineal no coin- ciden con las de la familia JK-O.

7. PROPIEDADES DE LAS AFINIDADES

Según hemos visto en el apartado 1 las afinidades pueden obtenerse por complementación de variables sobre el grupo lineal. Sea ---- $A \in GL_n(Z_2)$ y $(x_1 \ldots x_n) \in B^n$

$$B = A \oplus (x_1 \ldots x_n) \Longrightarrow B \in A_n(Z_2)$$

Como es sabido podemos representar la afinidad B mediante una matriz n+1xn+1 de la forma

$$\left[\begin{array}{ccc|c} & & & x_1 \\ & & & \cdot \\ & A & & \cdot \\ & & & \cdot \\ & & & x_n \\ \hline 0 & \cdot\;\cdot\;\cdot & 0 & 1 \end{array}\right] = B$$

Entre los elementos C, $B \in A_n(Z_2)$ podemos establecer una relación de equivalencia tal -- que

$$B \underset{2}{\simeq} C \Longleftrightarrow \exists V \in A_n(Z_2) \mid V^{-1} B\, V = C$$

Lema 4.- Sean A_1 y A_2 pertenecientes a la -- misma clase de $GL_n(Z_2)$, $x=(x_1 \ldots x_n) \in B^n$ y sea $A_1 \oplus x$ una afinidad -----------------------

$$\Longrightarrow \exists x' \in B^n \mid A_1 \oplus x \underset{2}{\simeq} A_2 \oplus x' .$$

Demostración:

Tomemos $V \in A_n(Z_2) \mid V = U \oplus (0 \ldots . 0)$ siendo $U \in GL_n(Z_2) \mid U^{-1} A_1\, U = A_2$

Sea B_1 la matriz correspondiente a la afinidad $A_1 \oplus x$

$$V^{-1} B_1\, V = (U^{-1} \oplus (0 \ldots 0))\ (A_1 \oplus (x_1 \ldots x_n))$$

$$(U \oplus (0 \ldots 0)) = (U^{-1}\, A_1\, U) \oplus U^{-1}(x_1 \ldots x_n) =$$

$$= A_2 \oplus x'$$

Teorema 5.- Las afinidades generadas por un elemento de una clase del grupo lineal son - independientes del representante elegido.

La demostración es trivial por aplicación -- del Lema 4.

Definición: Dados x e $y \in B^n$ y $M \in GL_n(Z_2)$ definimos la siguiente relación de equivalencia

$$x\, R_M\, y \Longleftrightarrow \exists z \in B^n \mid Mz \oplus x \oplus z = y$$

Teorema 6.- Para una $M \in GL_n(Z_2)$ dada, las - afinidades generadas por M con todos los vectores pertenecientes a la misma clase por la relación anterior son isomorfos.

Demostración: Dados

$M \in GL_n(Z_2)$ y $x,y \in B^n \mid x\, R_M\, y \;\; \exists V \in A_n(Z_2) \mid$

$$V^{-1} (M \oplus x)\, V = M \oplus y$$

Si $x\, R_M\, y \Longrightarrow \exists z \mid Mz \oplus x \oplus . z = y$, tomando $V = I \oplus z$

$$(I \oplus z)\ (M \oplus x)\ (I \oplus z) = M \oplus y \Longrightarrow$$

las afinidades $M \oplus x \underset{2}{\simeq} M \oplus y$ #

Ello significa que elegido el representante de una de las clases, $\underset{2}{\simeq}$, de $GL_n(Z\ )$ no es - necesaria la comprobación de las 2^n -1 traslaciones posibles. Será necesario exclusivamente la comprobación de las $\# \{B^n/R_M\}$ posibilidades.

8. GENERALIZACION AL CASO DET(A) = 0.

Consideremos el conjunto de matrices S = --- $= \{A \mid \forall i \sum a_{ij} \leqslant a_{ii} + 1\}$ con det A = 0. - La función F asociada a la matriz A es una - aplicación de $B^n \longrightarrow B^n$ que no es inyectiva ni exhaustiva.

De forma análoga al caso lineal estas matrices estarán caracterizadas por su polinomio característico $P(\lambda)$ y su descomposición en - polinomios elementales.

Sea $P(\lambda) = \lambda^n \oplus a_n \lambda^{n-1} \oplus \ldots \oplus a_2 \lambda \oplus a_1$ la expresión general del polinomio característico en el caso considerado $a_1 = 0$ ya que det $A = 0$, de manera que siempre podremos expresar $P(\lambda)$ de la forma

$$P_A(\lambda) = \lambda^s \; (\lambda^{n-s} \oplus a_n \; \lambda^{n-s-1} \oplus \ldots \oplus a_{s+1}) \text{ con}$$

$a_{s\ 1} \neq 0$

y de la aplicación del Teorema 3 resulta que A corresponde a composición de A_1 y A_2 con $A_2 \in GL_n(Z_2)$ y $A_1 \in S$ y es de la forma

$$A_1 = \begin{pmatrix} 0 & c_1 & 0 & 0 & \cdots \\ 0 & 0 & c_2 & 0 & \cdots \\ & & \ddots & & \\ & & & & \ddots \end{pmatrix} \quad c_i \in \{0,1\}$$

El valor de los c_i vendrá determinado por la descomposición en polinomios elementales de tal forma que si

$$Q_A(\lambda) = \lambda^r \; (P_A(\lambda) \; / \; \lambda^s)$$

mediante un cambio de base la matriz A podremos transformarla en otra matriz B de la forma

$$B = \left[\begin{array}{c|c|c} \begin{matrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & \\ 0 & \cdots & 0 & 1 \\ 0 & \cdots & 0 & 0 \end{matrix} & & \\ \hline & \begin{matrix} 0 & c_{s-r} & & \\ & 0 & c_{s-r-1} & \\ & & \ddots & \\ 0 & \cdots & 0 & c_s \\ 0 & \cdots & \cdots & 0 \end{matrix} & \\ \hline & & P_A(\lambda) \; / \lambda^s \end{array}\right]$$

De donde resulta que podemos obtener las clases de isomorfía JK - 0 no completos como composición iterativa de elementos completos y no completos que hayan aparecido para valores anteriores de <u>n</u>.

9. APLICACION A LA SINTESIS DE CONTADORES

Del estudio realizado en los apartados anteriores se deduce que el conjunto Γ_3, definido de forma análoga a Γ_2, coincide con el conjunto de funciones pertenecientes a $GL_n(Z_2)$. Por consiguiente, cualquier m.s.a. admite un representante cuyas funciones de entrada fi son de la forma

1) $fi = Q_1 +_2 Q_{i+1}$

2) $fi = Q_{i+1} \qquad \forall i = 1, \ldots, n \; ; \; Q_{n+1} = 0$

En el caso particular en que la m.s.a pertenezca a Γ_2 encontramos también un representante que corresponde a una T-matriz, siendo fi en este caso de la forma

1) $fi = Q_i +_2 Q_{i+1}$

2) $fi = Q_{i+1} \qquad \forall i = 1, \ldots, n-1.$

3) $fn = Q_1$

De las consideraciones anteriores se deduce que podemos sintetizar un contador lineal de longitud cualquiera por conexión de un número <u>n</u> (n = grado del polinomio) de módulos iguales del tipo.

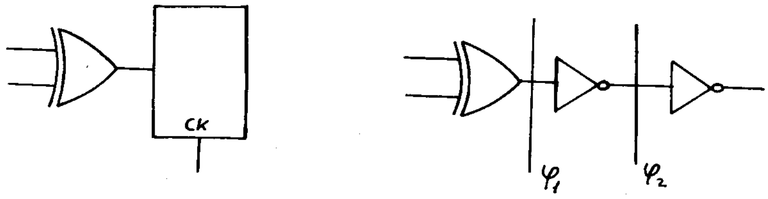

FIGURA 1. Módulo básico

Consideremos por ejemplo la matriz $A \in GL_n(Z)$

$$A = \begin{matrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{matrix}$$

con polinomio característico $P(\lambda) = \lambda^5 + \lambda^3 + 1$ y que corresponde a una m.s.a. cuya función estado siguiente $f = (f_1\ f_2\ f_3\ f_4\ f_5)$ se identifica con las filas de dicha matriz.

Debido a que $P(\lambda)$ es irreducible la forma canónica de Jacobson $\underset{2}{\simeq}$ con A es la siguiente matriz B.

$$B = \begin{matrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{matrix}$$

que corresponde a una m.s.a. cuyas funciones fi son:

$$\left.\begin{aligned} f1 &= Q_1^\Delta = Q_2 \\ f2 &= Q_2^\Delta = Q_1 +_2 Q_3 \\ f3 &= Q_3^\Delta = Q_4 \\ f4 &= Q_4^\Delta = Q_5 \\ f5 &= Q_5^\Delta = Q_1 \end{aligned}\right\}$$

Por otra parte $\lambda^5 + \lambda^3 + 1 = \lambda^3(\lambda +_2 1)^2 +_2 1$ admitiendo la T-matriz

$$T = \begin{matrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{matrix}$$

y las funciones correspondientes a la m.s.a. en este caso son:

$$\left.\begin{aligned} f1 &= Q_1 +_2 Q_2 \\ f2 &= Q_2 +_2 Q_3 \\ f3 &= Q_4 \\ f4 &= Q_5 \\ f5 &= Q_1 \end{aligned}\right\}$$

Utilizando el módulo base de la figura 1 para el diseño de las m.s.a. correspondientes a las matrices B y T obtenemos los diagramas lógicos indicados en las figuras 2 y 3

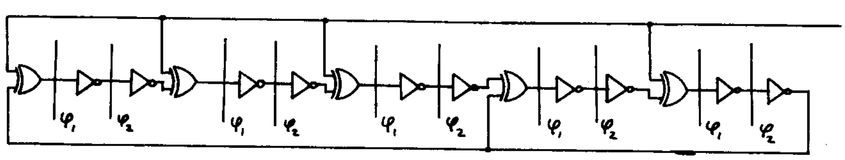

FIGURA 2. Forma canónica de Jacobson

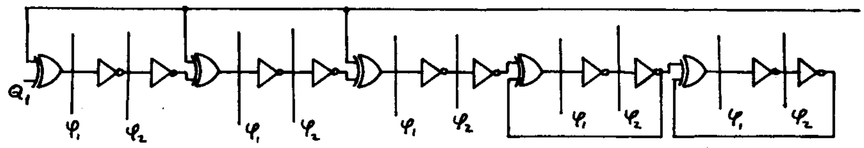

FIGURA 3. T-matrices

10. COMPARACION ENTRE LOS DOS METODOS.

La síntesis a partir de la descomposición canónica de Jacobson tiene la ventaja de ser siempre posible con un número de básculas igual al grado del menor polinomio cuya periodicidad sea la deseada. En cambio el hecho de que $a_{1n} \neq 0$ y que a_{1j} no sea en general nulo significa la necesidad de una línea de conexión interna desde el primero al último de los módulos básicos conectados lo que compromete por una parte la idoneidad de la realización desde el punto de vista de la superficie de silicio ocupada y por otra la posibilidad de utilizar módulos standard en la síntesis de contadores de longitudes de ciclo muy largas.

Si la implementación se realiza a partir de la forma de T-matriz el principal inconveniente reside en el hecho de que no se puede asegurar en todos los casos la existencia de una T-matriz de periodicidad K. ($T^K = I$) cuya dimensión coincide con el grado del menor polinomio de esta periodicidad. En cambio en este caso las interconexiones son locales lo que contribuye a una disminución de la superficie ocupada por el módulo básico y a la posibilidad de acoplamiento de módulos de este tipo para la síntesis de grandes longitudes.

11. BIBLIOGRAFIA

/1/ STONE H.S., "Discrete Mathematical structures and their applications", Science Research Associates Inc., Chicago 1973

/2/ STORY, HARRISON, REINHART, "Optimum state assignment for synchronous sequential circuits". IEEE Trans. on Comput. C-21, nº 12 (Dec. 1972).

/3/ DOLOTTA, T.A., McCLUSKEY, E.J., "The Coding of internal states of sequential circuits". IEEE Trans. on Computers, EC-13, pp 549-562 (1964).

/4/ J. AGUILO, E. VALDERRAMA, "On the digraph classification with 1-row unimodular matrices". IEEE Inter. Symposium on Circuits and Systems. Chicago. Marzo 1981.

/5/ E. VALDERRAMA, "Asignación de estados en máquinas sin lógica combinacional". Tesis Doctoral. (1979).

/6/ HARRISON M.A., "Counting theorems and their application to switching functions" A. Muckopadhyay, 1971., Academic Press.

/7/ R. GODIMENT, "Un cours d'Algèbre" ed. Hermann. Paris.

/8/ T. OSES, "Tratamiento formal de máquinas secuenciales autónomas y su aplicación a la integración de contadores" Tesis Doctoral. Dic. 1981.

12. NOTA.

La parte fundamental de este trabajo ha sido publicado ya en las 1as. Jornadas de Diseño Lógico. Barcelona 15-17 de Julio de 1981.