Sur la théorie du test des circuits digitaux : mesures de la confiance

Mireille Jocomino

THESE
présentée par

Mireille JACOMINO
née DANCET

Ingénieur E . N . S . I . E . G

pour obtenir le titre de DOCTEUR
de l'INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE
(arrêté ministériel du 5 juillet 1984)

Spécialité : Automatique

==========

Sur la Théorie du Test des Circuits Digitaux : Mesures de la Confiance

==========

Date de soutenance : 17 Février 1989.

Composition du jury :

Madame	S . GENTIL	Président
Messieurs	B. COURTOIS	
	R. DAVID	
	R. GERBER	Examinateurs
Madame	P . THEVENOD/FOSSE	

Thèse préparée au sein du Laboratoire d'Automatique de Grenoble

INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE

Président : Georges LESPINARD

Année 1988

Professeurs des Universités

BARIBAUD	Michel	ENSERG
BARRAUD	Alain	ENSIEG
BAUDELET	Bernard	ENSPG
BEAUFILS	Jean-Pierre	ENSEEG
BLIMAN	Samuel	ENSERG
BLOCH	Daniel	ENSPG
BOIS	Philippe	ENSHMG
BONNETAIN	Lucien	ENSEEG
BOUVARD	Maurice	ENSHMG
BRISSONNEAU	Pierre	ENSIEG
BRUNET	Yves	IUFA
CAILLERIE	Denis	ENSHMG
CAVAIGNAC	Jean-François	ENSPG
CHARTIER	Germain	ENSPG
CHENEVIER	Pierre	ENSERG
CHERADAME	Herve	UFR PGP
CHOVET	Alain	ENSERG
COHEN	Joseph	ENSERG
COUMES	André	ENSERG
DARVE	Félix	ENSHMG
DELLA-DORA	Jean-François	ENSIMAG
DEPORTES	Jacques	ENSPG
DESRE	Pierre	ENSEEG
DOLMAZON	Jean-Marc	ENSERG
DURAND	Francis	ENSEEG
DURAND	Jean-Louis	ENSIEG
FOGGIA	Albert	ENSIEG
FONLUPT	Jean	ENSIMAG
FOULARD	Claude	ENSIEG
GANDINI	Alessandro	UFR PGP
GAUBERT	Claude	ENSPG
GENTIL	Pierre	ENSERG
GREVEN	Hélène	IUFA
GUERIN	Bernard	ENSERG
GUYOT	Pierre	ENSEEG
IVANES	Marcel	ENSIEG
JAUSSAUD	Pierre	ENSIEG
JOUBERT	Jean-Claude	ENSPG
JOURDAIN	Geneviève	ENSIEG
LACOUME	Jean-Louis	ENSIEG
LESIEUR	Marcel	ENSHMG
LESPINARD	Georges	ENSHMG
LONGEQUEUE	Jean-Pierre	ENSPG
LOUCHET	François	ENSIEG
MASSE	Philippe	ENSIEG
MASSELOT	Christian	ENSIEG
MAZARE	Guy	ENSIMAG
MOREAU	René	ENSHMG
MORET	Roger	ENSIEG
MOSSIERE	Jacques	ENSIMAG
OBLED	Charles	ENSHMG
OZIL	Patrick	ENSEEG
PARIAUD	Jean-Charles	ENSEEG
PERRET	René	ENSIEG
PERRET	Robert	ENSIEG
PIAU	Jean-Michel	ENSHMG
POUPOT	Christian	ENSERG
RAMEAU	Jean-Jacques	ENSEEG
RENAUD	Maurice	UFR PGP
ROBERT	André	UFR PGP
ROBERT	François	ENSIMAG
SABONNADIERE	Jean-Claude	ENSIEG
SAUCIER	Gabrielle	ENSIMAG
SCHLENKER	Claire	ENSPG
SCHLENKER	Michel	ENSPG
SERMET	Pierre	ENSERG
SILVY	Jacques	UFR PGP
SIRYES	Pierre	ENSHMG
SOHM	Jean-Claude	ENSEEG
SOLER	Jean-Louis	ENSIMAG
SOUQUET	Jean-Louis	ENSEEG
TROMPETTE	Philippe	ENSHMG
VEILLON	Gérard	ENSIMAG
ZADWORNY	François	ENSERG

Personnes ayant obtenu le diplôme

D'HABILITATION A DIRIGER DES RECHERCHES

BECKER	Monique
BINDER	Zdeneck
CHASSERY	Jean-Marc
CHOLLET	Jean-Pierre
COEY	John
COLINET	Catherine
COMMAULT	Christian
CORNUEJOLS	Gérard
COULOMB	Jean-Louis
DALARD	Francis
DANES	Florin
DEROO	Daniel
DIARD	Jean-Paul
DION	Jean-Michel
DUGARD	Luc
DURAND	Madeleine
DURAND	Robert
GALERIE	Alain
GAUTHIER	Jean-Paul
GENTIL	Sylviane
GHIBAUDO	Gérard
HAMAR	Sylvaine
HAMAR	Roger
LADET	Pierre
LATOMBE	Claudine
LE CORREC	Bernard
MADAR	Roland
MULLER	Jean
NGUYEN TRONG	Bernadette
PASTUREL	Alain
PLA	Fernand
ROUGER	Jean
TCHUENTE	Maurice
VINCENT	Henri

CHERCHEURS DU C.N.R.S

Directeurs de recherche 1ère Classe

CARRE	René	LANDAU	Ioan
FRUCHART	Robert	VACHAUD	Georges
HOPFINGER	Emile	VERJUS	Jean-Pierre
JORRAND	Philippe		

Directeurs de recherche 2ème Classe

ALEMANY	Antoine	KLEITZ	Michel
ALLIBERT	Colette	KOFMAN	Walter
ALLIBERT	Michel	KAMARINOS	Georges
ANSARA	Ibrahim	LEJEUNE	Gérard
ARMAND	Michel	LE PROVOST	Christian
BERNARD	Claude	MADAR	Roland
BINDER	Gilbert	MERMET	Jean
BONNET	Roland	MICHEL	Jean-Marie
BORNARD	Guy	MUNIER	Jacques
CAILLET	Marcel	PIAU	Monique
CALMET	Jacques	SENATEUR	Jean-Pierre
COURTOIS	Bernard	SIFAKIS	Joseph
DAVID	René	SIMON	Jean-Paul
DRIOLE	Jean	SUERY	Michel
ESCUDIER	Pierre	TEODOSIU	Christian
EUSTATHOPOULOS	Nicolas	VAUCLIN	Michel
GUELIN	Pierre	WACK	Bernard
JOUD	Jean-Charles		

Personnalités agréées à titre permanent à diriger des travaux de recherche (décision du conseil scientifique)

ENSEEG

CHATILLON	Christian	SARRAZIN	Pierre
HAMMOU	Abdelkader	SIMON	Jean-Paul
MARTIN GARIN	Régina		

ENSERG

BOREL	Joseph

ENSIEG

DESCHIZEAUX	Pierre	PERARD	Jacques
GLANGEAUD	François	REINISCH	Raymond

ENSHMG

ROWE	Alain

ENSIMAG

COURTIN	Jacques

EFP

CHARUEL	Robert

C.E.N.G

CADET	Jean	NIFENECKER	Hervé
COEURE	Philippe	PERROUD	Paul
DELHAYE	Jean-Marc	PEUZIN	Jean-Claude
DUPUY	Michel	TAIEB	Maurice
JOUVE	Hubert	VINCENDON	Marc
NICOLAU	Yvan		

Laboratoires extérieurs :

C.N.E.T

DEVINE	Rodericq	MERCKEL	Gérard
GERBER	Roland	PAULEAU	Yves

****

****

***

Faisant le geste vif d'écarter les nuages
Elle touche enfin terre, au sortir de ses astres.

J . Supervielle

A mes mari Marie

Avant – propos

Le travail présenté dans ce mémoire a été effectué au Laboratoire d'Automatique de Grenoble (L.A.G) de l'Ecole Nationale Supérieure d'Ingénieurs Electriciens de Grenoble (E.N.S.I.E.G), sous la direction de Monsieur R. David, Directeur de Recherche CNRS, et dans le cadre d'un contrat avec le Centre National d'Etudes des Télécommunications (CNET/CNS).

Avant toute chose je souhaite exprimer ma reconnaissance à Monsieur R. David grâce à qui j'ai vécu une première expérience professionnelle très enrichissante. Vous m'avez accordé toute votre confiance en travaillant avec moi dans un véritable esprit de collaboration, j'en ai été trés honorée et vous en remercie. Je veux rendre hommage ici à votre compétence et votre dynamisme qui font de vous un véritable chef d'équipe et qui sont le moteur de nombreuses activités.

Je tiens à remercier Madame S. Gentil, Professeur à l'Institut National Polytechnique de Grenoble, d'avoir accepté de présider le jury de cette thèse.

Mes remerciements vont également à Monsieur R. Gerber, responsable de la division "Conception de Circuits Intégrés" au CNET/CNS, pour avoir accepté la lourde charge de rapporteur.

Je voudrais aussi exprimer ma gratitude à P. Thévenod-Fosse, Chargée de Recherche CNRS, de l'intérêt qu'elle a porté à mes recherches et pour lesquelles elle a su provoquer l'attention. A ses côtés j'ai fait mes premiers pas dans la communauté scientifique internationale, sa présence attentive m'a permis de m'intégrer rapidement. Bien qu'elles soient épisodiques nos rencontres sont le ciment d'une amitié que je tiens à lui exprimer ici.

Je remercie vivement Monsieur B. Courtois, Directeur de Recherche CNRS, pour l'intérêt qu'il a manifesté vis-à-vis de mes travaux. Sa contribution à ce jury a été très appréciée.

J'exprime mes sincères remerciements au personel du CNET avec lequel j'ai collaboré et en particulier à Monsieur J-L Rainard pour l'attention qu'il a portée à mes recherches et les conseils avisés qu'il m'a prodigués.

Je suis très sensible à l'intérêt que porte Monsieur I.D. Landau, Directeur du L.A.G., à notre axe de recherche et je l'en remercie.

Je ne saurais refermer cette page sans m'adresser à vous, mes amis du L.A.G.

Je voudrais souligner le dévouement du personel administratif qui a su m'apporter le soutien nécessaire dans la réalisation de ce mémoire.

Enfin je tiens à saluer mes co-équipiers pour l'attention dont ils sont capables. J'ai été très sensible au climat de fraternité qu'ils ont su créer grâce à leurs qualités humaines. Qu'ils trouvent ici l'expression de ma profonde amitié.

Sommaire

Sommaire

Chapitre 1

Introduction

Le test d'un circuit digital consiste à appliquer en entrée de ce circuit une séquence de test et à observer sa sortie. Si aucune erreur n'est apparue, le circuit est reconnu bon, sinon il est reconnu défectueux. Le résultat "bon/mauvais" dépend des paramètres suivants :

1) le *rendement de fabrication.* Si le circuit est bon et que le dispositif de test n'introduit pas d'erreur (ce qui est le plus souvent le cas) alors le circuit est reconnu bon.

2) la *séquence de test* et en particulier la capacité de celle-ci à faire apparaître une erreur en sortie d'un circuit lorsqu'une faute est présente.

3) les *fautes qui peuvent affecter le circuit.* La séquence de test appliquée fait apparaître une erreur pour certaines fautes si l'une d'elles est présente dans le circuit sous test. Si une autre faute est présente le circuit est, à tort, reconnu bon.

4) le *dispositif d'observation* de la sortie du circuit testé. Si la séquence de sortie est "compactée" avant d'être observée alors une erreur présente dans cette séquence peut être masquée.

5) la *fiabilité du dispositif de test.* Si le dispositif de test introduit des erreurs, un circuit bon peut être à tort reconnu défectueux.

Si le test était parfait le résultat ne dépendrait que de l'état du circuit. Tous les circuits bons seraient reconnus bons et tous les circuits défectueux seraient reconnus mauvais. Les différentes méthodes de test développées ne permettent pas de distinguer parfaitement les circuits bons des circuits défectueux. En particulier certains circuits défectueux sont reconnus bons. Les chercheurs qui travaillent sur ce sujet s'intéressent, le plus souvent, à un aspect du dispositif de test. Les uns développent des méthodes de conception de séquences de test, les autres étudient les performances de certains observateurs.

L'objectif de notre travail n'est pas de proposer une méthode de test des circuits digitaux, mais de mesurer la confiance que l'on peut accorder au résultat du test. Soit une expérience de test, c'est-à-dire 1) une séquence de test appliquée à un ensemble de circuits qui peuvent être affectés d'une faute, suivie de 2) l'observation, directe ou non, de la sortie de ces circuits, 3) l'observation conduit au résultat "bon" ou "mauvais" du test. Le problème que nous cherchons à résoudre se pose en ces termes : celui qui se fie au résultat de cette expérience peut-il être sûr de l'état des circuits auxquels il s'intéresse ?

Les deux grandeurs suivantes permettent d'estimer la qualité du test appliqué : d'une part la proportion de circuits correctement testés parmi tous les circuits testés et d'autre part la

proportion de circuits réellement bons parmi tous les circuits reconnus bons. Ces deux proportions ne peuvent être connues qu'*a posteriori* éventuellement. L'étude que nous développons dans ce mémoire a pour but de définir des mesures *a priori* de la qualité d'un test. On parlera de *confiance dans le test.*

Dans un premier temps nous donnons une définition formelle des deux mesures de confiance dans les circuits testés qui correspondent aux deux mesures de qualité définies ci-dessus. A partir de ces définitions on montre que ces deux mesures sont des fonctions croissantes de la capacité de la méthode de test à détecter un circuit défectueux. En effet plus la méthode de test permet de détecter de circuits défectueux plus le nombre de circuits reconnus bons est petit, et plus le test est performant. Il résulte que la mesure de la confiance dans les circuits testés passe par la mesure de la confiance dans la méthode de test. Nous définissons 4 mesures de la confiance dans la méthode de test. On montre qu'une seule d'entre elles permet de calculer la confiance dans les circuits testés, c'est la *mesure la plus significative.* L'étude comparative des différentes mesures sur le plan de la "qualité" et de la difficulté d'évaluation (chapitre 3) conduit à l'observation suivante : il existe d'une part une mesure très précise qui est difficile à évaluer et d'autre part une borne inférieure facile à obtenir. Nous proposons une nouvelle approche (chapitre 4) qui permet d'estimer la confiance dans la méthode de test à partir de plusieurs mesures faciles à estimer. Cette méthode consiste à n'étudier de façon précise que les éléments du circuit les plus difficiles à tester car ce sont eux qui déterminent la confiance dans le test. Cette approche permet de calculer deux bornes de la confiance dans la méthode de test. Ces deux bornes peuvent être très proches l'une de l'autre.

Les résultats que nous obtenons sont valables quelle que soit la séquence de test (déterministe ou aléatoire) et quel que soit l'analyseur de signature utilisé. De plus ils s'étendent facilement au cas du test compact statistique (cas où la signature n'est connue que par ses propriétés statistiques).

L'étude de la confiance dans le test que nous avons développée et qui fait l'objet de la partie A de ce mémoire, a permis de mettre en évidence l'influence de différents paramètres comme le rendement de fabrication, la nature des fautes et leur fréquence d'apparition dans le circuit, et la fiabilité du dispositif de test.

Dans la partie B nous appliquerons les résultats obtenus dans la partie A à un microprocesseur CMOS à test intégré réalisé au CNET/CNS : le MTI, microprocesseur à test intégré. Après l'étude détaillée du test des fautes les plus difficiles à tester dans un circuit CMOS nous mesurerons la confiance dans le test du MTI. La nouvelle approche, que nous décrivons dans le chapitre 4, permet d'estimer à 10^{-5} près la confiance dans la méthode de test implantée dans le MTI, sous réserve de certaines hypothèses.

Partie A

Aspect théorique

Chapitre 2

Test des circuits digitaux

Dans ce chapitre les différentes caractéristiques d'un test sont présentées. Les notions de test aléatoire, test déterministe, test compact, analyse de signature, test autonome sont définies.

2 . 1 . Introduction

De nos jours un très grand nombre de systèmes sont commandés à partir de circuits intégrés. Du pilotage d'une navette spatiale à la programmation d'une calculatrice, les exemples sont variés. Dans tous les cas le bon fonctionnement du système dépend du bon fonctionnement du circuit qui le commande. C'est ce qui explique l'intérêt et l'**importance** du test des circuits digitaux. Par ailleurs la mise au point du test est rendue de plus en plus difficile par la complexité croissante des circuits intégrés.

On peut distinguer deux types de circuits : les *bons* qui réalisent la fonction pour laquelle ils ont été conçus, et les circuits *défectueux* qui, pour certaines configurations des entrées, ne réalisent pas la fonction pour laquelle ils ont été conçus.

Une **défaillance** est un défaut physique qui est à l'origine du mauvais fonctionnement d'un circuit défectueux. Un contact mal pris, une coupure, un canal trop étroit sont des exemples de défaillance.

Une **faute** est un modèle de mauvais fonctionnement dû à une défaillance. Au niveau du transistor le collage ouvert et le collage fermé sont deux modèles de fautes. Au niveau d'une porte logique le collage à 0 ou à 1 est le modèle de faute le plus souvent utilisé.

Une **erreur** est une valeur incorrecte due à la présence d'une faute dans le circuit. La figure 2.1 illustre ces différentes notions.

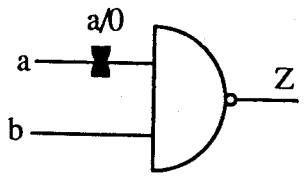


Figure 2.1 : Porte Nand défectueuse

L'entrée "a" collée à 0, notée **a/0**, signifie que la branche "a" est à la valeur 0 quelle que soit la valeur de la variable "a". Le collage a/0 est *une faute*. Si on applique sur a et b le vecteur d'entrée ab = 11 la sortie Z prend la valeur logique 1, alors que la valeur attendue est 0. *Une erreur*

est apparue en sortie de la porte défectueuse. Si on applique un des vecteurs ab = 01 ou 00 ou 10 la sortie Z de la porte défectueuse prend la valeur logique 1 qui est la valeur attendue. Aucune erreur n'apparaît. Le vecteur ab = 11 est appelé **vecteur de test** pour la faute a/0. Si la faute a/0 est présente dans le circuit sous test et que le vecteur de test 11 est appliqué, alors une erreur apparaît en sortie du circuit. On dit que la faute a/0 a été **testée**.

La mise en oeuvre du test d'un circuit se fait en fonction d'**hypothèses de fautes**. On dresse une liste de fautes qui peuvent affecter le circuit en se limitant à celles qui sont jugées les plus fréquentes, ou que l'on sait étudier.

2 . 2 . Différents types de test

Trois types de test sont généralement appliqués à un circuit logique :

Le test paramétrique consiste à vérifier les caractéristiques statiques d'un circuit. Certaines grandeurs électriques sont mesurées : courant et tension sur les entrées, sur les sorties ...

Le test dynamique permet de vérifier l'évolution des grandeurs électriques en fonction du temps. Les temps de commutation ainsi que les plages de stabilité des sorties sont observées.

Le test fonctionnel permet de vérifier de bon comportement logique du circuit.

Notre travail concerne le *test fonctionnel* uniquement. Le principe du test fonctionnel est illustré à la figure 2.2. Une séquence d'entrée, appelée **séquence de test**, est appliquée au circuit sous test (en abrégé CST). La séquence de sortie observée est comparée à la séquence de sortie obtenue à partir d'un circuit bon. Cette séquence de **référence** peut être obtenue soit par simulation et elle est ensuite enregistrée (figure 2.2a), soit en appliquant la séquence de test en même temps au circuit sous test et à un circuit réputé bon (figure 2.2b). La séquence de sortie observée peut être soit la séquence de sortie sous test appelée **réponse** soit une **image compacte** de cette réponse (figure 2.2c). On parlera d'**observation compacte**. L'image compacte de la réponse est disponible en sortie de l'observateur lorsque la séquence de test a été entièrement appliquée.

Si la séquence de sortie est identique à la séquence de référence, c'est-à-dire qu'aucune erreur n'est apparue en sortie du CST, alors le circuit sous test est *reconnu bon* sinon il est *reconnu défectueux*.

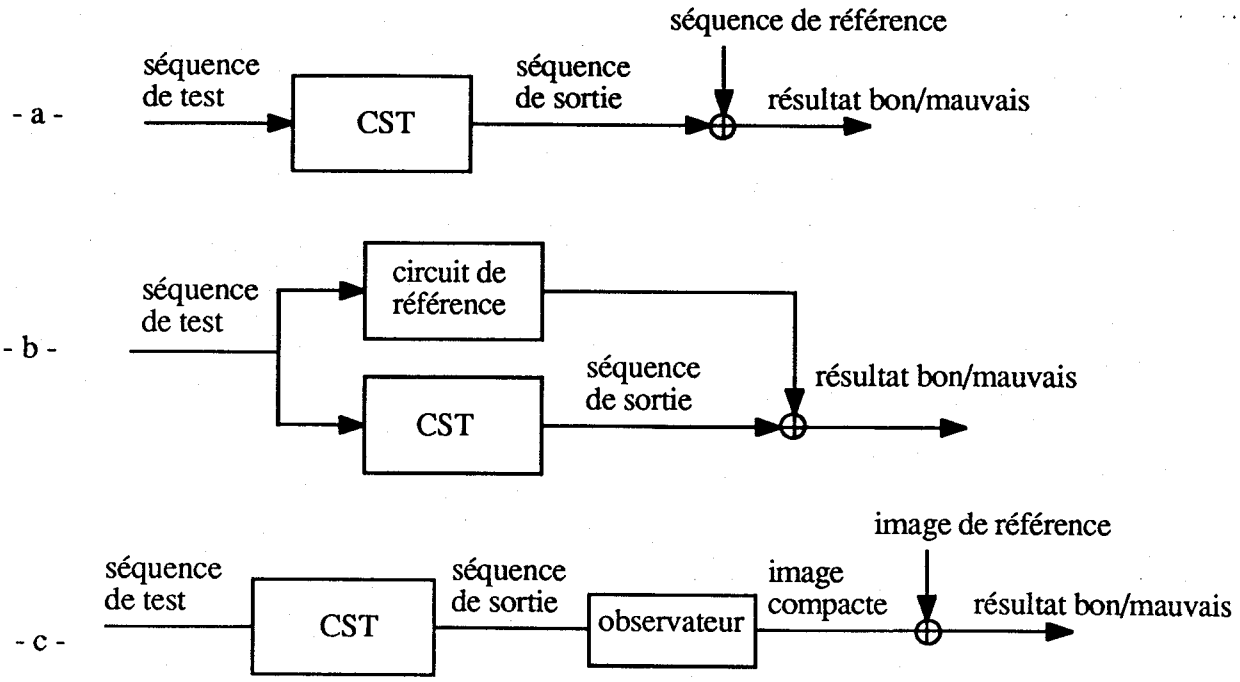


Figure 2.2 : Principe d'une expérience de test

2 . 3 . Nature de la séquence de test

On distingue deux types de test suivant la nature de la séquence de test appliquée.

Le test déterministe consiste 1) à rechercher un ensemble de vecteurs qui permet de tester toutes les fautes retenues dans les hypothèses puis 2) à appliquer ces vecteurs en entrée du CST. Une séquence de test déterministe est entièrement connue. Cette méthode se prête mal à la complexité croissante des circuits car elle entraîne une élaboration de plus en plus pénible de la séquence de test. L'analyse du circuit est faite à l'aide de simulateurs adaptés.

Le test aléatoire consiste à appliquer une séquence aléatoire en entrée du CST. La séquence de test n'est pas connue. On ne connait que ses propriétés statistiques. Pour faciliter la génération des vecteurs de test, un test aléatoire est souvent réalisé à partir d'une séquence de test *pseudo-aléatoire*. Une séquence pseudo-aléatoire est une séquence déterministe qui possède les proprétés statistiques d'une séquence aléatoire [David 86]. Cette séquence est reproductible ce qui n'est pas le cas d'une séquence aléatoire non enregistrée. Une séquence pseudo-aléatoire est très facile à générer. L'étude préalable à réaliser pour mettre en oeuvre un test aléatoire consiste à calculer le nombre de vecteurs aléatoires (**longueur de test**) à appliquer pour détecter un circuit

défectueux.

A partir d'une liste de fautes possibles on sait en test déterministe si la séquence de test appliquée teste ou non chacune de ces fautes. La proportion de fautes testées, appelé **taux de couverture de fautes**, caractérise la capacité de la séquence de test à détecter un circuit défectueux. Cette grandeur est la mesure de confiance utilisée par tous les auteurs qui traitent du test déterministe. En test aléatoire la longueur de test est le paramètre qui détermine la capacité de la séquence de test à détecter un circuit défectueux. A partir d'un *critère de confiance* on calcule la longueur de test (en test déterministe la confiance est calculée *a posteiriri*). Le critère le plus souvent utilisé est appelé **faute de pire cas** [Rault 71]. Il consiste à prendre comme hypothèse que tous les circuits défectueux sont affectés de la faute la plus difficile à tester. Nous verrons dans le chapitre 3 que la mesure de confiance dans le test peut être envisagée indépendemment de la méthode de test utilisée.

On peut souligner le fait que le schéma général d'un test fonctionnel est celui de la figure 2.2b. En effet avec une séquence aléatoire il n'existe pas de séquence de sortie de référence enregistrée puisque la séquence de test n'est pas reproductible. Toutefois on connait les propriétés statistiques de la réponse d'un circuit pour toute séquence de test possible. Ces propriétés constituent une image compacte de référence de la réponse. On peut donc envisager un test aléatoire compact sans circuit de référence.

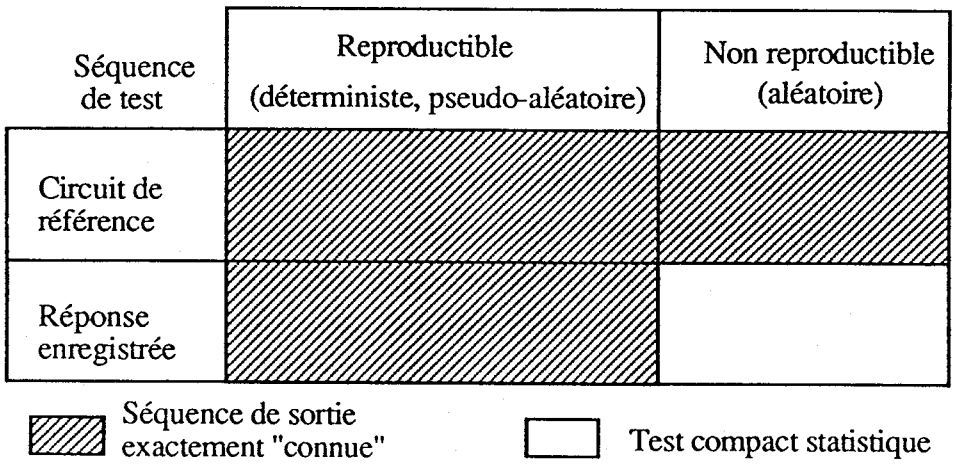


Figure 2.3 : Différents types d'observations compactes

On peut distinguer deux types d'observations compactes suivant que l'image de référence est ou non exactement connue. Si la séquence de test est reproductible (déterministe ou pseudo-aléatoire ou aléatoire enregistré) l'image de référence est exactement connue. On parle alors d'**analyse de signature**. Si la séquence de test n'est pas reproductible (aléatoire) l'image de

référence représente une propriété statistique de la réponse d'un circuit bon. Cette propriété est vérifiée en moyenne, c'est-à-dire sur un grand nombre de séquences appliquées mais pas sur chaque réalisation d'une séquence de test. En d'autres termes un circuit bon ne conduit pas toujours à l'image de référence, cela dépend de la séquence de test appliquée. On parle dans ce cas de **test compact statistique**. Du point de vue de la confiance de test, le test compact statistique est un cas très particulier. Le chapitre 5 de ce mémoire est consacré à l'étude de la confiance de test lorsque la réponse du CST est compactée.

Le tableau de la figure 2.3 illustre les différents cas possibles [David 79a], [Robinson 87].

2 . 4 . Mise en oeuvre

Les différentes méthodes de test que nous avons présentées peuvent être mises en oeuvre de manière différente. On peut distinguer deux types d'implantation suivant que le dispositif de test est externe au circuit testé ou qu'il est intégré.

2 . 4 . 1 . Test externe

Le générateur de séquences de test et le système d'observation (compactage et comparaison) sont extérieurs au circuit. Ils constituent le **testeur**. Cette implantation est largement utilisée pour le test de fin de fabrication mais elle permet difficilement de tester un circuit en maintenance, c'est-à-dire lorsqu'il est installé sur le site d'utilisation.

2 . 4 . 2 . Test autonome

Le générateur de séquences de test et le système d'observation sont implantés dans le circuit. Si le test est pris en compte au niveau de la conception du circuit, on peut l'intégrer sans entraîner une trop grande augmentation de surface du circuit. La **testabilité** d'un circuit caractérise la facilité à le tester. Il existe différents critères de testabilité [Agrawal 82], [Keiner 77], [Savir 83]. L'*observabilité* et la *commandabilité* sont deux de ces critères [Mc Cluskey]. Plusieurs approches ont été développées qui permettent de concevoir un circuit en vue du test [Williams 82].

On peut distinguer deux types de test autonome selon qu'il est en ligne ou hors ligne. Dans le test en ligne, encore appelé **autotest**, il n'y a pas de séquence de test à proprement parler. La séquence d'entrée en fonctionnement sert simultanément de séquence de test. L'ensemble des sorties correctes du circuit est un ensemble codé. La détection d'une faute correspond à l'apparition d'une sortie qui n'appartient pas à l'ensemble des codes possibles [Anderson 73], [David 79b],

[Nicolaidis 86]. Ce dispositif de test permet de dire à tout instant si la sortie est correcte ce qui n'implique pas que le circuit soit sans faute.

Le dispositif de test autonome hors ligne, appelé **test intégré**, comprend un générateur de séquences de test, un système d'observation et un sélecteur de **mode test** implanté dans le circuit. En mode test les éléments fonctionnels du circuit travaillent à partir de données issues du générateur de séquences de test et les sorties sont observées pour conduire au résultat du test. En **mode fonctionnement** les entrées primaires servent de données et les sorties sont directement observées.

Remarques 2.1 : 1) L'application d'une séquence déterministe suppose que l'on enregistre la séquence de test préalablement calculée. Cette méthode est très coûteuse en place mémoire. Un générateur de séquences pseudo-aléatoires occupe peu de place et permet de travailler à haute fréquence si nécessaire.

2) L'utilisation d'un circuit de référence n'est évidemment pas compatible avec un test autonome, sauf dans le cas très particulier où le circuit nominal contient des éléments redondants.

□

Quelle que soit la nature de la séquence de test, quelle que soit la mise en oeuvre du dispositif de test, on peut décomposer une expérience de test en 3 parties :

- l'application d'une séquence de test,
- l'apparition ou non d'une erreur,
- l'observation de la réponse du circuit.

L'observation de la réponse du circuit conduit au **résultat du test**. Ce résultat peut prendre 2 valeurs : **"bon"** ou **"mauvais"**. Il ne correspond malheureusement pas toujours à l'état réel du circuit. Dans le premier cas le circuit va être utilisé, dans le second il sera éliminé. A partir de cette description générale d'une expérience de test, on peut caractériser de plusieurs manières la confiance que l'on peut accorder au résultat du test. L'étude que nous allons développer est indépendante de la nature et de la mise en oeuvre de l'expérience de test.

La description des différentes caractéristiques du test d'un circuit digital faite dans ce chapitre illustre la diversité des tests qui peuvent être réalisés. Le formalisme que nous allons développer par la suite s'applique à tous les dispositifs de test.

Chapitre 3

Etude de la confiance dans un test

Dans ce chapitre deux mesures de la confiance dans l'état "bon ou mauvais" d'un circuit testé sont définies de façon formelle. Ces deux mesures s'écrivent en fonction du rendement de fabrication et de la capacité de la séquence de test à détecter un circuit défectueux. La variable qui permet de mesurer cette capacité est difficile à obtenir en pratique. Nous donnons la définition formelle de trois autres mesures qui permettent d'estimer la performance de la séquence de test. Ces quatre mesures de la confiance dans la séqence de test sont comparées suivant deux critères : la précision et la difficulté d'obtention.

3 . 1. Introduction

Dans notre vie quotidienne nous sommes amenés à faire des choix. Pour nous guider il existe des tests en tous genres. Prenons l'exemple d'un chef d'entreprise qui souhaite diversifier son activité. Pour ce faire il désire s'entourer de collaborateurs compétents. Après avoir publié ses offres d'emplois un grand nombre de candidats se présentent. Tous n'apporteront pas le même service à l'entreprise. Les divers tests et entretients d'embauche ont pour but de déceler les talents qui contribueront à la croissance de l'entreprise. Le résultat de ces tests détermine les candidats qu'il faut engager. Il est primordial pour le chef d'entreprise de connaître le degré de confiance qu'il peut accorder aux résultats des tests pour ne pas risquer d'embaucher des personnes qui ne répondraient pas à son attente. S'il s'avère que le test n'est pas approprié il peut en envisager d'autres. Le résultat du test est important seulement s'il permet de distinguer les bons candidats des moins bons, pour l'entreprise.

Cet exemple nous montre qu'il est important de mesurer la confiance dans un test. Ce chapitre est consacré à l'étude de la confiance dans le test des circuits digitaux. Nous allons illustrer les principales notions à partir du schéma de la figure 3.1. Soit W le nombre de *circuits à tester* (on suppose dans tout ce qui suit que W est un grand nombre). Parmi ces W circuits G fonctionnent correctement, on dira qu'ils sont *bons* et D ne réalisent pas la fonction pour laquelle ils ont été conçus, on dira qu'ils sont *défectueux*. On a W = G + D. L'**expérience de test** étudiée dans ce chapitre consiste à appliquer aux W circuits *une séquence de test* (déterministe ou aléatoire) et à comparer la séquence de sortie obtenue à une séquence réputée correcte. Le dispositif de test a pour but de séparer les G circuits bons des D circuits défectueux. Naturellement cette séparation est imparfaite. Pour D_p circuits défectueux le processus de test ne fait pas apparaître de mauvais fonctionnement. Ces circuits sont, *à tort, reconnus bons* et *acceptés*. Par ailleurs D_f circuits défectueux sont *refusés* après détection d'un mauvais fonctionnement. On a $D = D_p + D_f$. On suppose que tous les circuits bons sont correctement testés, ce qui est le cas en pratique.

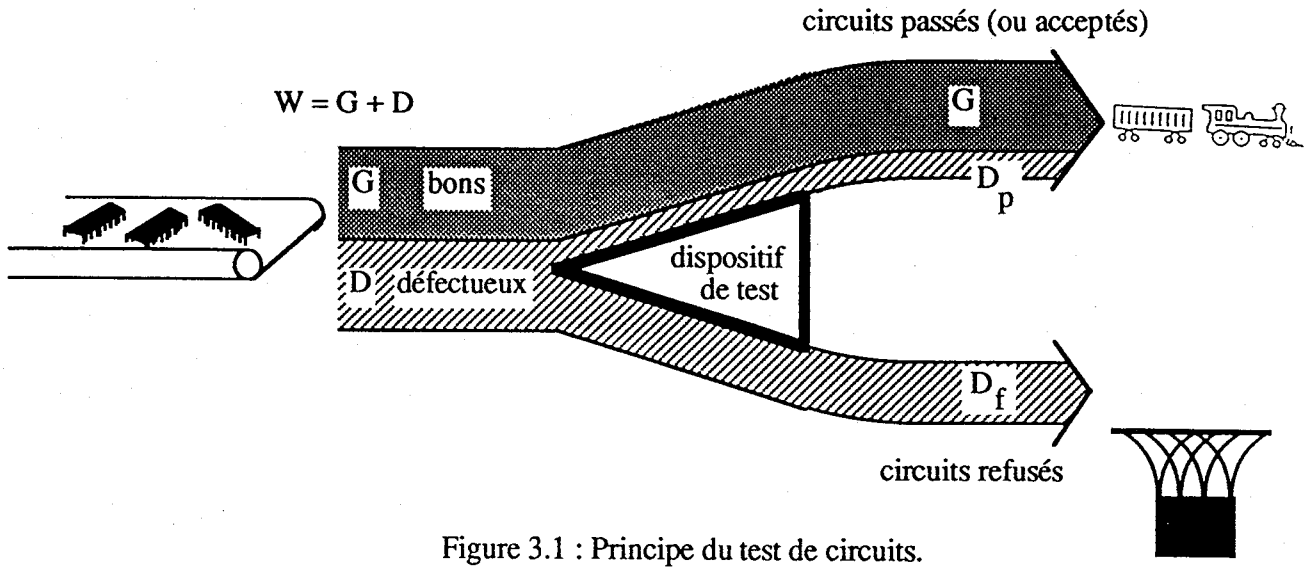


Figure 3.1 : Principe du test de circuits.

Remarque 3.1 : Cette hypothèse pourrait être mise en défaut si le dispositif de test était défectueux par exemple. On se place ici dans le cas où le dispositif de test est beaucoup plus fiable que les circuits testés. On verra dans la partie B consacrée à l'étude d'un microprocesseur expérimental qu'un circuit avec test intégré peut aussi rentrer dans cette hypothèse.

□

A l'issue d'une expérience de test on a $G + D_p$ **circuits acceptés** qui sont considérés comme bons (on parlera aussi de **circuits passés**) et D_f **circuits refusés** qui sont défectueux. Les D_p circuits défectueux acceptés caractérisent l'imperfection du test. Plus D_p est petit, meilleur est le résultat du test.

A partir de ce schéma de test deux indicateurs permettent de mesurer la **qualité du test** réalisé sur un échantillon de W circuits.

Le rapport $(G+D_f) / W$ est la *proportion de circuits correctement testés*. Cette mesure caractérise la qualité du test pour chaque circuit testé. Elle intéresse *le fabricant* des circuits testés.

Le rapport $G / (G+D_p)$ est la *proportion des circuits passés* qui sont réellement *bons*. Cette mesure caractérise la qualité du test pour les seuls circuits reconnus bons et qui vont être utilisés. Cette mesure intéresse *l'utilisateur* des circuits testés.

Ces deux rapports ne peuvent être calculés qu'*a posteriori* si toutefois on peut dénombrer les D_p circuits défectueux passés.

Lorsqu'un dispositif de test est mis en oeuvre on veut généralement connaître ses performances *a priori*. On parlera alors de **confiance dans le test.** Pour chacune des deux mesures de qualité que nous venons de présenter on peut définir une mesure de confiance correspondante.

La *confiance moyenne dans les circuits testés* notée C_t, est la probabilité de tester correctement un circuit. Lorsque le nombre W de circuits testés est grand, C_t est égal à $(G+D_f) / W$.

La *confiance moyenne dans les circuits passés* notée C_a, est la probabilité qu'un circuit passé soit bon. Lorsque W est grand C_a est égal à $G / (G+D_p)$.

Remarque 3.2 : Ces deux mesures C_t et C_a représentent l'espérance mathématique des rapports $(G+D_f) / W$ et $G / (G+D_p)$ respectivement. Ce sont les valeurs moyennes que l'on obtiendrait sur un grand nombre de réalisations d'une expérience de test.

□

Dans le schéma de test que nous avons retenu aucun circuit bon ne peut être refusé. Il est donc clair intuitivement que pour un nombre G donné de circuits bons la qualité du test est déterminée par la *capacité de la séquence de test à détecter un circuit défectueux*. On appellera **confiance dans la séquence de test** cette capacité. En d'autres termes plus grande est la proportion D_f / D de circuits défectueux bien testés, plus sûr est le test. Nous verrons dans la partie 3.3 que les deux mesures de la confiance dans les circuits testés C_t et C_a sont des fonctions croissantes de la *couverture des circuits défectueux* notée P_a. Cette mesure de la confiance dans la séquence de test est la probabilité de détecter un circuit défectueux sachant qu'il est défectueux. C'est aussi la valeur moyenne pour un grand nombre d'expériences de test du rapport D_f / D.

Après avoir défini explicitement le lien qui permet de passer d'une proportion de circuits testés ($(G+D_f) / W$ ou $G / (G+D_p)$ ou D_f / D) à une mesure de confiance (C_t ou C_a ou P_a) nous prendront la liberté dans la suite de ce mémoire de confondre ces deux notions dans des remarques informelles. On suppose que le nombre de circuits testés est très grand.

On rencontre dans la littérature trois autres mesures de la confiance dans la séquence de test. Il nous a paru intéressant de développer une analyse comparative des différentes mesures possibles afin de dégager l'intérêt de chacune d'entre elles. Voyons de manière informelle comment chacune de ces mesures s'inscrit dans le schéma de test décrit à la figure 3.1.

La première mesure est la *probabilité de la couverture complète* notée P_c. C'est la probabilité que tous les circuits défectueux soient refusés. On a $P_c = Pr [D_p = 0]$.

La *probabilité minimum de test* notée P_m, est la probabilité minimum de détecter un circuit défectueux sachant qu'il est défectueux. En d'autres termes P_m est la probabilité minimum pour que n'importe quel circuit parmi les D circuits défectueux soit parmi les D_f circuits refusés.

La présentation de cette mesure met en évidence le fait que tous les circuits défectueux

n'ont pas la même probabilité d'être détectés par la séquence de test appliquée. Si c'était le cas on aurait $P_m = P_a$. Un circuit défectueux est affecté d'une des fautes de l'ensemble $F = \{f_1, f_2, ..., f_M\}$ l'*ensemble de fautes prescrit*. La probabilité de détecter un circuit défectueux est déterminée par la faute qui l'affecte. C'est en fait la probabilité que la séquence d'entrée teste la faute présente dans le circuit.

La *couverture de fautes espérée* notée P_E, est la moyenne arithmétique du nombre de fautes de F testées par la séquence d'entrée. Cette mesure de la confiance dans la séquence de test caractérise la capacité de la séquence d'entrée à tester une faute de F et non pas directement à détecter un circuit défectueux. Elle ne peut, sans autre hypothèse, être définie par rapport aux données du schéma de la figure 3.1.

Les trois autres mesures de la confiance dans la séquence de test (P_a, P_c, P_m) peuvent également être définies par rapport aux fautes prescrites. Les propriétés statistiques de l'ensemble de fautes prescrit permettent de calculer les différentes mesures. Ceci fera l'objet des définitions formelles énoncées aux paragraphes suivants.

Le travail que nous allons développer est indépendant de la séquence de test appliquée (déterministe ou aléatoire). Le test aléatoire des circuits est le cas générique. Une approche probabiliste du problème permet d'associer à chaque mesure une relation de définition valable dans tous les cas. Néanmoins nous nous attacherons dans la partie 3.5 à appliquer les résultats obtenus dans les parties précédentes au cas du test déterministe.

3 . 2 . Hypothèses et notations

Le dispositif de test que nous étudions est décrit à la figure 3.2.

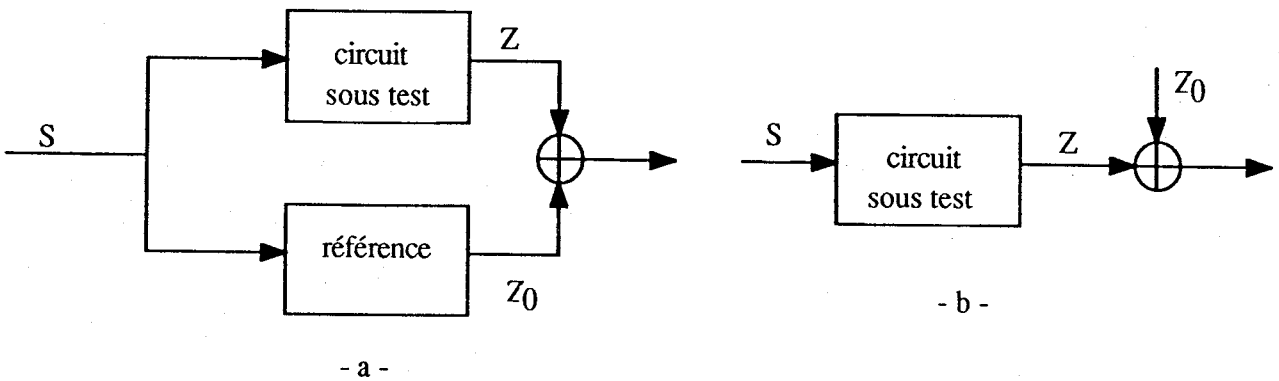


Figure 3.2 : Dispositif de test
a - Test avec circuit de référence b - Test avec référence enregistrée

Dans le cas général du test aléatoire la séquence d'entrée n'est pas reproductible. Il faut donc appliquer la séquence d'entrée à la fois au circuit sous test et à un circuit réputé sans faute (Fig. 3.2a). Ce dispositif de test peut également être utilisé en test déterministe pour éviter d'enregistrer la réponse qui est souvent longue (plusieurs milliers de bits). Lorsque le test est autonome on compare la séquence de sortie du circuit sous test à la séquence correcte enregistrée (Fig.3.2b).

3 . 2 . 1 . Hypothèses

Avant que le test proprement dit ne commence une séquence d'initialisation est appliquée au circuit sous test (en abrégé CST) s'il est séquentiel afin de le conduire dans un état connu, s'il est correct ; l'état initial pouvant être inconnu sinon. Le circuit sous test (CST) peut être affecté d'**une faute f_i** de l'ensemble $F = \{f_1, f_2, ..., f_M\}$ l'**ensemble de fautes prescrit**. Le circuit est alors **défectueux**. Si le circuit est **sans faute** on dira qu'il est affecté de la faute f_0.

Remarque 3.3 : L'introduction de cette faute f_0, qui peut paraître arbitraire, permet d'une part d'avoir le même modèle pour tous les circuits testés, bons ou défectueux, et d'autre part d'alléger les notations. On écrira f_0 pour circuit sans faute.

□

Hypothèse 3.1 : Les fautes f_i sont **exclusives**. Une faute multiple est un élément de F.

□

La séquence d'entrée **S**, dite **séquence de test**, est alors appliquée au CST. Soit X_j un **vecteur d'entrée** du CST. La séquence de test est une suite ordonnée de L vecteurs $S = X_1X_2...X_L$. Si le test est déterministe, la séquence S est exactement connue, et on sait pour chaque faute de F si elle est ou non testée par S. Si le test est aléatoire, on ne connait que les propriétés statistiques de la séquence de test. La capacité de cette séquence à détecter chacune des fautes de F est alors une probabilité.

La séquence de sortie du CST notée **Z** est appelée la **réponse** du CST. La réponse d'un circuit affecté de la faute f_i est notée Z_i. Si le circuit est sans faute sa réponse est Z_0.

Hypothèse 3.2 : Un circuit sans faute ne peut pas produire une réponse incorrecte.

□

La **probabilité d'occurrence** d'une faute f_i notée **Pr** $[f_i]$, est la probabilité que la

faute f_i affecte le CST. Lorsque le nombre W de circuits est grand Pr [f_i] est égal à la proportion de circuits testés affectés de la faute f_i. La probabilité d'occurrence de la faute f_0, c'est-à-dire la **probabilité d'occurrence d'un circuit sans faute**, est le **rendement de fabrication** noté **Y = Pr [f_0]**. Lorsque W est grand, Y est égal au rapport G / W.

La confiance dans la séquence de test caractérise la capacité de la séquence de test à détecter un circuit défectueux. En d'autres termes c'est la probabilité de détecter un circuit défectueux sachant qu'il est défectueux. Cette probabilité dépend de la faute présente dans le CST sachant qu'une faute de F est présente. Les paramètres qui sont donc réellement utiles sont les **probabilités conditionnelles d'occurrence** notée **Pr [f_i/F], i = 1, ..., M**. Pour une faute f_i la probabilité Pr [f_i/F] est la probabilité que le CST soit affecté de la faute f_i sachant qu'il est défectueux. Lorsque W est grand c'est la proportion de circuits affectés de la faute f_i parmi les D circuits défectueux. Les notations présentées jusque là nous permettent d'écrire la relation suivante :

$$\Pr [f_i] = (1-Y) \Pr [f_i/F] , \qquad \text{pour } i = 1, ..., M \qquad (3.1)$$

Par la suite on sera amené à travailler essentiellement sur les circuits défectueux. Le paramètre important sera alors la fréquence d'apparition d'une faute dans un circuit défectueux, c'est-à-dire sa probabilité d'occurrence conditionnelle. Par abus de langage on parlera de probabilité d'occurrence de la faute f_i pour désigner la probabilité d'occurrence conditionnelle Pr [f_i/F].

Le **profil d'occurrence** noté Ω, est le vecteur composé des probabilités d'occurrence conditionnelles des fautes f_i. C'est-à-dire :

$$\Omega = (\Pr [f_1/F], \Pr [f_2/F], ..., \Pr [f_M/F])$$

Soit Ω_e le profil d'occurrence lorsque toutes les fautes de F sont équiprobables :

$$\Omega_e = (1/M, ...,1/M)$$

3 . 2 . 2 . Notions de base

Comme nous l'avons déjà souligné, le résultat "bon/mauvais" d'un test ne correspond pas toujours à l'état du circuit testé. Si aucune erreur n'apparaît en sortie du CST lorsque la séquence S est appliquée, c'est-à-dire $\mathbf{Z = Z_0}$, on dit que le circuit est **passé**. Sinon il est **refusé**. Par ailleurs on dira que le **résultat du test est juste** si :

soit 1) le circuit est sans faute et passé

soit 2) le circuit est défectueux et refusé

Remarque 3.4 : Le cas 2) peut s'écrire simplement : le circuit est refusé. D'après l'hypothèse 3.2

refusé implique défectueux. Dans la partie 5.3 de ce mémoire cette hypothèse n'est plus imposée c'est pourquoi nous avons conservé la définition dans la cas général.

□

La capacité de la séquence de test à tester un circuit est caractérisée par la probabilité que la faute f_i, qui affecte la CST soit testée par S. Soit $\mathbf{P_T(f_i)}$, la **probabilité de test** de la faute f_i. C'est la probabilité

1) que la séquence de test S fasse apparaître une erreur en sortie d'un CST lorsque la faute f_i est présente, si f_i appartient à F.

2) qu'aucune erreur n'apparaisse en sortie du CST si la faute f_0 est présente.

En d'autres termes la probabilité de test de la faute f_i est la probabilité que le résultat du test soit juste lorsque f_i est présente dans le CST.

$$P_T(f_i) = Pr\,[\text{résultat du test est juste} / f_i] \qquad (3.2)$$

Propriété 3.1 : La probabilité de test de la faute f_i peut s'écrire :

a) $P_T(f_0) = 1$

b) $P_T(f_i) = Pr\,[Z \neq Z_0/f_i] = Pr\,[Z_i \neq Z_0]$, pour $i = 1, ..., M$

Démonstration : a) D'après l'hypothèse 3.2 aucun circuit bon ne peut être refusé donc tous les circuits bons sont correctement testés. Donc :

$$Pr\,[f_0] = Pr\,[Z = Z_0 / f_0] = 1$$

b) Si la faute f_i est présente dans le circuit sous test, le résultat du test est juste si une erreur apparaît en sortie de ce circuit lorsqu' on applique la séquence S ($Z \neq Z_0$). On a donc pour $i \neq 0$: $P_T(f_i) = Pr\,[Z \neq Z_0/f_i] = Pr\,[Z_i \neq Z_0]$

□

On utilisera souvent la notation explicite $Pr\,[Z_i \neq Z_0]$ pour écrire la probabilité de test de la faute f_i.

Lorsque la séquence de test est déterministe la probabilité de tester la faute f_i est égale à 1 si S contient au moins un vecteur (pour un circuit combinatoire) qui teste la faute f_i et à 0 sinon.

Lorsque la séquence de test est aléatoire $P_T(f_i)$ dépend de la longueur de test appliquée. Nous allons écrire la relation qui permet de calculer $P_T(f_i)$ pour un circuit combinatoire. On suppose que la longueur de test est très grande et que tous les vecteurs de test appliqués ont la même probabilité de tester f_i. Soit d_i la probabilité de test par un vecteur de la faute f_i. Pour un circuit combinatoire testé par une séquence aléatoire dans laquelle les vecteurs d'entrée X_j sont

équiprobables d_i est la proportion des vecteurs d'entrée qui testent f_i. Avec ces hypothèses on a :

$$P_T(f_i) = 1 - (1 - d_i)^L \qquad (3.3)$$

Ces différentes notions vont nous permettre de donner une définition formelle des mesures présentées au paragraphe 3.1.

3 . 3 . Confiance dans les circuits testés

Les deux parties qui suivent sont consacrées à la définition formelle des différentes mesures qui permettent d'évaluer la confiance dans la séquence de test. Ces définitions s'appliquent à tout circuit (combinatoire ou séquentiel), à toute séquence de test (déterministe ou aléatoire) et à tout ensemble de fautes prescrit.

Définition 3.1 : La confiance moyenne dans les circuits testés pour une séquence de test S, notée C_t, est la probabilité que le résultat du test soit juste lorsque la séquence S est appliquée.

$$C_t = \Pr[\text{le résultat du test est juste}]$$

□

Cette mesure est nouvelle à notre connaissance.

Le résultat du test est juste si 1) soit un circuit est passé et sans faute, 2) soit un circuit est défectueux et refusé. On peut donc écrire :

$$C_t = \Pr[f_0 \text{ et } Z = Z_0] + \Pr[F \text{ et } Z \neq Z_0] \qquad (3.4)$$

Calculons chacun de ces deux termes :

1) $\Pr[f_0 \text{ et } Z = Z_0] = \Pr[f_0] \Pr[Z = Z_0/f_0]$. D'après l'hypothèse 3.2 aucun circuit sans faute n'est refusé. On a donc $\Pr[Z = Z_0/f_0] = 1$ et

$$\Pr[f_0 \text{ et } Z = Z_0] = \Pr[f_0] = Y$$

2) $\Pr[F \text{ et } Z \neq Z_0] = \Pr[F] \Pr[Z \neq Z_0/F]$. La probabilité $\Pr[F]$ est la probabilité que le CST soit défectueux donc $\Pr[F] = 1 - Y$

D'où on peut écrire :

$$C_t = Y + (1-Y) \Pr[Z \neq Z_0/F] \qquad (3.5)$$

La confiance moyenne dans les circuits testés s'écrit en fonction du rendement de fabrication Y et de la variable $\Pr[Z \neq Z_0/F]$. C'est la probabilité qu'un circuit défectueux soit refusé. En d'autres termes c'est l'espérance mathématique de la proportion D_f / D de circuits

défectueux refusés. Cette probabilité caractérise la capacité de la séquence de test à détecter un circuit défectueux.

Définition 3.2 : La **couverture des circuits défectueux** de la séquence S notée $\mathbf{P_a}$, est la probabilité que la séquence S teste la faute qui affecte le CST sachant que ce circuit est défectueux.

$$P_a = Pr\,[Z \neq Z_0/F] \tag{3.6}$$

□

L'ensemble F contient M fautes, $F = \{f_1, f_2, ..., f_M\}$ qui lorsque le circuit est défectueux, constituent un système complet d'événements. On peut donc écrire :

$$P_a = Pr\,[Z \neq Z_0/f_1]\,Pr\,[f_1/F] + ... + Pr\,[Z \neq Z_0/f_M]\,Pr\,[f_M/F]$$

D'après la propriété 3.1b, P_a peut s'écrire sous les deux formes suivantes :

$$P_a = Pr\,[Z_1 \neq Z_0]\,Pr\,[f_1/F] + ... + Pr\,[Z_M \neq Z_0]\,Pr\,[f_M/F] \tag{3.7}$$

$$P_a = P_T(f_1)\,Pr\,[f_1/F] + ... + P_T(f_M)\,Pr\,[f_M/F] \tag{3.8}$$

On retrouve sous cette forme la notion de *fonction de distribution de la latence d'erreur* (nombre de vecteurs de test appliqués avant détection) pour un ensemble de fautes définie par Shedletsky dans [Shedletsky 77] dans le cas du test aléatoire. Dans [Wagner 84] les auteurs définissent la *confiance pondérée de test* dans le cas du test pseudo-aléatoire. Dans ces deux articles seuls les circuits combinatoires sont étudiés.

A partir de l'équation (3.5) et de la définition 3.2 on obtient la propriété suivante :

Propriété 3.2 : La confiance moyenne dans les circuits testés est une fonction du rendement de fabrication et de la couverture des circuits défectueux.

$$C_t = Y + (1 - Y)\,P_a \tag{3.9}$$

□

Sous cette forme on retrouve les deux types de circuits qui sont bien testés : Y représente les circuits sans faute et (1 - Y) P_a représente les circuits défectueux (1 - Y) qui sont détectés (P_a).

Remarque 3.5 : A partir de la propriété 3.1 et des équations (3.8) et (3.9) on peut écrire :

$$C_t = P_T(f_0)\,Pr\,[f_0] + (1 - Y)\,P_T(f_1)\,Pr\,[f_1/F] + ... + (1 - Y)\,P_T(f_M)\,Pr\,[f_M/F]$$

En utilisant l'équation (3.1) on obtient :

$$C_t = P_T(f_0)\ Pr\ [f_0] + P_T(f_1)\ Pr\ [f_1] + ... + P_T(f_M)\ Pr\ [f_M]$$

Sous cette forme il est clair que C_t mesure la confiance obtenue sur l'ensemble des circuits testés : les circuits sans faute et les circuits défectueux. On voit bien que c'est une mesure *a priori* basée sur les propriétés statistiques de l'échantillon testé.

□

Définition 3.3 : La **confiance moyenne dans les circuits passés** pour la séqunce de test S notée C_a, est la probabilité qu'un circuit passé soit sans faute lorsque S est appliquée:

$$C_a = Pr\ [f_0 / Z = Z_0]$$

□

Propriété 3.3 : La confiance moyenne dans les circuits passés s'écrit en fonction du rendement de fabrication et de la couverture des circuits défectueux.

$$C_a = \frac{Y}{Y + (1 - Y)(1 - P_a)}$$

Démonstration : On peut écrire :

$$Pr\ [f_0] = Y = Pr\ [Z = Z_0]\ Pr\ [f_0/Z = Z_0] + Pr\ [Z \neq Z_0]\ Pr\ [f_0/Z \neq Z_0]$$

D'après l'hypothèse 3.2 on a $Pr\ [f_0/Z \neq Z_0] = 0$. D'où on peut écrire :

$$Pr\ [f_0/Z = Z_0] = \frac{Pr\ [f_0]}{Pr\ [Z = Z_0]} = C_a$$

avec $Pr\ [Z = Z_0] = Pr\ [f_0]\ Pr\ [\ Z = Z_0/\ f_0] + Pr\ [F]\ Pr\ [Z = Z_0/F]$. D'après l'hypothèse 3.2 on a $Pr\ [\ Z = Z_0/\ f_0] = 1$. D'où :

$$Pr\ [Z = Z_0] = Y + (1 - Y)\ Pr\ [Z = Z_0/F] = Y + (1 - Y)(1 - P_a)$$

□

Sous cette forme on retrouve au dénominateur les deux types de circuits passés : Y représente les circuits bons et $(1 - Y)(1 - P_a)$ représente les circuits défectueux $(1 - Y)$ passés $(1 - P_a)$.

La même notion apparaît dans [Williams 81] sous le nom de *niveau de défaut* . Les auteurs supposent que toutes les fautes simples sont équiprobables. La probabilité d'une faute multiple peut être calculée à partir des fautes simples qui la composent. A partir de ces hypothèses le niveau de défaut est exprimé en fonction du rendement de fabrication et du taux de couverture des fautes simples.

Les propriétés 3.2 et 3.3 permettent de décrire l'influence sur la confiance dans les circuits testés d'une part des circuits bons et d'autre part de la capacité de la séquence de test à

détecter un circuit défectueux.

Théorème 3.1 : Pour tout circuit, pour toute séquence de test et pour tout ensemble de fautes prescrit on a :

a) $C_t \geq P_a$, et $C_t > P_a$ si et seulement si $Y > 0$ et $P_a < 1$

b) $C_t \geq C_a \geq Y$, et $C_t > C_a$ si $Y < 1$ et $0 < P_a < 1$

c) C_t et C_a sont des fonctions croissantes de P_a pour tout Y tel que $0 < Y < 1$

Démonstration : Soient les expressions de C_t et C_a en fonction Y et P_a :

Propriété 3.2 $$C_t = Y + (1 - Y)\, P_a$$

Propriété 3.3 $$C_a = \frac{Y}{Y + (1 - Y)\,(1 - P_a)}$$

a) $\mathbf{C_t \geq P_a}$ **:** A partir de la propriété 3.2 on a $C_t - P_a = Y\,(1 - P_a)$. Comme Y et P_a sont des probabilités on a $C_t - P_a \geq 0$, et $C_t - P_a = 0$ si et seulement si $Y = 0$ ou $P_a = 1$.

b) $\mathbf{C_t \geq C_a \geq Y}$ **:** D'après la propriété 3.2 on a :

$$C_t - Y = (1 - Y)\, P_a \geq 0.$$

D'après la propriété 3.3 on a :

$$C_a - Y = \frac{Y\, P_a\, (1 - Y)}{Y + (1 - Y)\,(1 - P_a)} \geq 0$$

On a également :

$$C_t - C_a = \frac{P_a\, (1 - Y)^2 (1 - P_a)}{Y + (1 - Y)\,(1 - P_a)} \geq 0$$

On a de plus $C_t = C_a$ si $Y = 1$ ou $P_a = 0$ ou $P_a = 1$.

c) $\mathbf{C_t}$ **et** $\mathbf{C_a}$ **sont des fonctions croissantes de** $\mathbf{P_a}$ **:** Pour $0 < Y < 1$ on a :

$$\frac{dC_t}{dP_a} = 1 - Y > 0 \quad \text{et} \quad \frac{dC_a}{dP_a} = \frac{Y\,(1 - Y)}{(Y + (1 - Y)(1 - P_a))^2} > 0$$

□

Ce théorème démontre formellement les relations intuitives qui lient ces différentes mesures.

La proportion de circuits bien testés (C_t) est au moins égale

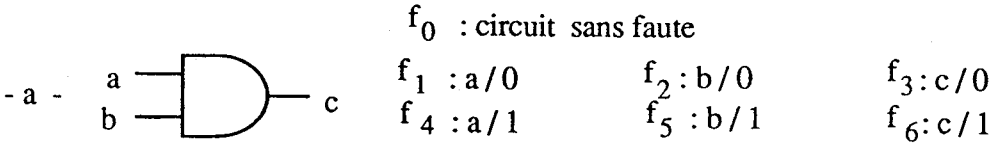
1) à la proportion de circuits bons car tous les circuits bons sont bien testés (Th. 3.1b)

2) à la proportion de circuits défectueux bien testés (P_a) (Th. 3.1a). Si la séquence de test ne détecte aucun circuit défectueux alors la proportion des circuits passés bien testés (C_a) est égale à la proportion de circuits bons Y. La capacité de la séquence de test à détecter un circuit

défectueux permet de diminuer le nombre de circuits passés donc d'augmenter la proportion de circuits passés bien testés (Th. 3.2b et c)

Aucun circuit refusé n'est mal testé donc la proportion des circuits bien testés (refusés ou passés et bons) est supérieure ou égale à la proportion des circuits passés et bons (Th. 3.1b).

Les mesures de la confiance dans les circuits testés sont utiles d'un point de vue pratique. Les deux mesures proposées C_t et C_a sont des fonctions croissantes de la *couverture des circuits défectueux*. C'est donc cette dernière mesure de la confiance dans la séquence de test qui *permet de mesurer la confiance dans les circuits testés*. Lorsqu'une séquence de test, déterministe ou aléatoire, est appliquée à un circuit la performance de cette séquence de test doit être évaluée par sa couverture des circuits défectueux. Malheureusement ce n'est pas toujours possible du fait de la connaissance nécessaire du CST et en particulier du profil d'occurrence. D'autres mesures de la confiance dans la séquence de test ont été définies et sont souvent utilisées. Il nous paraît intéressant de comparer ces mesures avec P_a qui est la mesure la plus significative à la lumière de ce qui précède.



ab =	X1 00	X2 01	X3 10	X4 11	Pr [f_i]
f_0					0.88
f_1				X	0.01
f_2				X	0.01
f_3				X	0.01
f_4		X			0.03
f_5			X		0.03
f_6	X	X	X		0.03

- b -

⇒

d_i	Pr [f_i /F] c-a-d Ω
0,25	0.0833
0,25	0.0833
0,25	0.0833
0,25	0.25
0,25	0.25
0,75	0.25

- c -

Figure 3.3 : Exemple de circuit combinatoire.
a - Porte ET et fautes prescrites. b - Ensemble des données. c - Données déduites.

Nous nous proposons d'illustrer les différentes définitions formelles de ce chapitre par des calculs sur un exemple très simple : le test par une séquence aléatoire de longueur L d'une porte

ET à deux entrées (Fig. 3.3). Les quatre vecteurs d'entrée sont équiprobables. On suppose que le circuit peut être affecté par un collage simple. Soit F = $\{f_1, f_2, f_3, f_4, f_5, f_6\}$ = {a/0, b/0, c/0, a/1,b/1, c/1}(Fig. 3.3a). Les vecteurs qui détectent chaque faute ainsi que la probabilité d'occurrence de chaque faute sont présentés à la figure 3.3b. Par exemple la faute f_1 est détectée par le vecteur X_4 = ab = 11, et la probabilité que f_1 soit présente dans le CST est égale à 0,01. C'est-à-dire que 1% des circuits testés sont affectés de la faute f_1. On a en particulier Y = Pr $[f_0]$ = 0,88 c'est-a-dire que 88% des circuits testés sont sans faute. A partir des données de la figure 3.3b on peut calculer les valeurs de la figure 3.3c. Pour la faute f_1 par exemple d'après l'équation (3.1) on a :

$$\Pr[f_1/F] = \frac{\Pr[f_1]}{1 - Y} = 0{,}0833$$

C'est-à-dire que 8,33% des circuits défectueux sont affectés de la faute f_1. Cette faute ne peut être détectée que par un seul vecteur d'entrée. On a donc

$$d_1 = \frac{1}{4}$$

A partir du tableau de la figure 3.3c et de l'équation (3.3) on peut calculer :

$$P_T(f_1) = P_T(f_2) = P_T(f_3) = P_T(f_4) = P_T(f_5) = 1 - \left(1 - \frac{1}{4}\right)^L = 1 - \left(\frac{3}{4}\right)^L$$

$$P_T(f_6) = 1 - \left(1 - \frac{3}{4}\right)^L = 1 - \left(\frac{1}{4}\right)^L$$

A partir de ces différents paramètres : probabilités de test et d'occurrence de chaque faute de F, on peut calculer pour cet exemple la couverture des circuits défectueux. L'équation (3.8) permet d'écrire :

$$P_a = \Pr[f_1/F]\left(1 - \left(\frac{3}{4}\right)^L\right) + \Pr[f_2/F]\left(1 - \left(\frac{3}{4}\right)^L\right) + \Pr[f_3/F]\left(1 - \left(\frac{3}{4}\right)^L\right)$$
$$\Pr[f_4/F]\left(1 - \left(\frac{3}{4}\right)^L\right) + \Pr[f_5/F]\left(1 - \left(\frac{3}{4}\right)^L\right) + \Pr[f_6/F]\left(1 - \left(\frac{1}{4}\right)^L\right)$$

$$P_a = (\Pr[f_1/F] + \Pr[f_2/F] + \Pr[f_3/F] + \Pr[f_4/F] + \Pr[f_5/F])\left(1 - \left(\frac{3}{4}\right)^L\right) + \Pr[f_6/F]\left(1 - \left(\frac{1}{4}\right)^L\right)$$

Pour L = 4 on trouve $\mathbf{P_a = 0{,}762}$.

Grâce aux propriétés 3.2 et 3.3 le calcul de la confiance dans les circuits testés est immédiat à partir du calcul de P_a.

Pour notre exemple on a :

$$C_t = Y + (1 - Y)\,P_a = 0{,}88 + 0{,}12\,P_a$$

$$C_a = \frac{Y}{Y + (1 - Y)(1 - P_a)} = \frac{0{,}88}{0{,}88 + 0{,}12\,(1 - P_a)}$$

Pour L = 4 on trouve $\mathbf{C_t = 0{,}971}$ et $\mathbf{C_a = 0{,}968.}$

Les valeurs de P_a, C_t et C_a en fonction de la longueur de test sont représentées à la figure 3.4.

3 . 4 . Mesures classiques de la confiance dans la séquence de test

Cette partie est consacrée à la définition formelle des mesures usuelles de la confiance dans la séquence de test. Les propriétés générales qui lient ces différentes mesures à P_a en particulier seront ensuite démontrées.

3 . 4 . 1 . Mesures

a - Probabilité de la couverture complète :

Définition 3.4 : La **probabilité de la couverture complète** pour la séquence de test S notée $\mathbf{P_c}$, est la probabilité que S teste chaque faute de F.

$$P_c = \Pr\,[\,(Z_1 \neq Z_0) \text{ et } \ldots \text{ et } (Z_M \neq Z_0)\,]$$

□

Cette mesure a été implicitement utilisée par Tellez et David dans [Tellez 74] lorsqu'ils considèrent la *probabilité de tester chaque faute*. Savir et Bardell dans [Savir 84] utilisent la *probabilité d'échapper* qui est égale à 1 - P_c. Cette notion est également citée dans [Wagner 87] sous le nom de *couverture de fautes à 100%*. Malayia et Yang dans [Malayia 84] définissent le *nombre espéré de vecteurs aléatoires qui produira la couverture complète* comme une mesure de la testabilité d'un circuit.

Exemple : On peut voir à la figure 3.3-b que les vecteurs X_2, X_3 et X_4 sont nécessaires et suffisants pour tester toutes les fautes prescrites. On a donc

$P_c = \Pr\,[X_2 \text{ et } X_3 \text{ et } X_4 \text{ appartiennent à S}]$

$P_c = \Pr\,[X_2 \in S]\ \Pr\,[X_3 \in S / X_2 \in S]\ \Pr\,[X_4 \in S / X_2 \in S \text{ et } X_3 \in S]$

Calculons chaque terme de ce produit :

$$\Pr\,[X_2 \in S] = 1 - \Pr\,[X_2 \notin S] = 1 - (3/4)^L$$

Si $X_2 \in S$ alors au moins un des L vecteurs de S est X_2. Donc X_3 ne peut alors être que l'un des L-1 autres vecteurs. On a alors :

$$\Pr [X_3 \in S / X_2 \in S] = 1 - \Pr [X_3 \notin \text{un ensemble de (L-1) vecteurs}] = 1 - (3/4)^{L-1}$$

De même on calcule :

$$\Pr [X_4 \in S / X_2 \in S \text{ et } X_3 \in S] = 1 - \Pr [X_4 \notin \text{un ensemble de (L-2) vecteurs}] = 1 - (3/4)^{L-2}$$

Pour $L \leq 2$ on a $P_c = 0$.

Pour $L \geq 3$ on a $P_c = [\, 1 - (3/4)^L]\, [\, 1 - (3/4)^{L-1}]\, [\, 1 - (3/4)^{L-2}]$.

Pour L = 4 on trouve $\mathbf{P_c = 0{,}321}$

La valeur de P_c en fonction de la longueur L de la séquence de test est représentée à la figure 3.4.

b - Couverture de fautes espérée

Définition 3.5 : La **couverture de fautes espérée** de la séquence S notée $\mathbf{P_E}$, est la moyenne arithmétique du nombre de fautes de F testées par S.

$$P_E = \frac{\Pr[Z_1 \neq Z_0] + \ldots + \Pr[Z_M \neq Z_0]}{M}$$

□

Cette notion est usuelle en test déterministe. Nous montrerons dans la partie 3.5 que P_E est égale dans ce cas au *taux de couverture de fautes*.

Dans [Malaiya 84] et dans [Wagner 87] les auteurs utilisent cette notion pour calculer la confiance dans un test aléatoire. Ils ne traitent que les circuits combinatoires et utilisent la notion de profil de détection pour définir cette grandeur. Le *profil de détection* d'un ensemble de fautes est le vecteur $(\Pi_1, \Pi_2, \ldots)$ dans lequel Π_i est le nombre de fautes dans F qui sont testées par i vecteurs d'entrée. Ils étudient dans un premier temps la couverture de fautes espérée en fonction de la longueur de test puis la contribution de chaque faute à la couverture de fautes espérée.

Exemple : A partir des probabilités de test $P_T(f_i) = \Pr [Z_i \neq Z_0]$ on peut écrire :

$$P_E = \frac{1}{6}\left(5\left(1 - \left(\frac{3}{4}\right)^L\right) + \left(1 - \left(\frac{1}{4}\right)^L\right)\right)$$

Pour L = 4 on trouve $\mathbf{P_E = 0{,}736}$

La valeur de P_E en fonction de la longueur L est représentée à la figure 3.4.

c - Probabilité minimum de test

Définition 3.6 : La **probabilité minimum de test** pour la séquence S notée $\mathbf{P_m}$, est la probabilité minimum de tester la faute qui affecte le circuit sous test sachant que ce circuit est défectueux.

$$P_m = \min (Pr [Z_1 \neq Z_0], \ ..., Pr [Z_M \neq Z_0])$$

□

La probabilité minimum de test est la probabilité de tester la faute la plus difficile à tester. Plusieurs auteurs l'ont utilisée sous le nom de *faute de pire cas*. Cette notion est la plus utilisée dans le cas du test aléatoire où elle prend tout son sens. En effet en test déterministe la probabilité minimum de test est égale à la probabilité de la couverture complète (nous le montrerons dans la partie 3.5).

Cette mesure a été introduite dès 1971 par Rault dans [Rault 71]. David et Blanchet qui l'ont appelée *qualité de test* ont montré dans [David 76] que c'était une mesure plus pertinente que la probabilité de la couverture complète alors appelée *qualité de détection.*

Exemple : A partir des probabilités de test des fautes prescrites on a :

$$P_m = \min \left(\left(1 - \left(\frac{3}{4}\right)^L \right), \left(1 - \left(\frac{1}{4}\right)^L \right) \right) = \left(1 - \left(\frac{3}{4}\right)^L \right)$$

Pour L = 4 on trouve $\mathbf{P_m = 0{,}683.}$

La valeur de P_m en fonction de la longueur L est représentée à la figure 3.4.

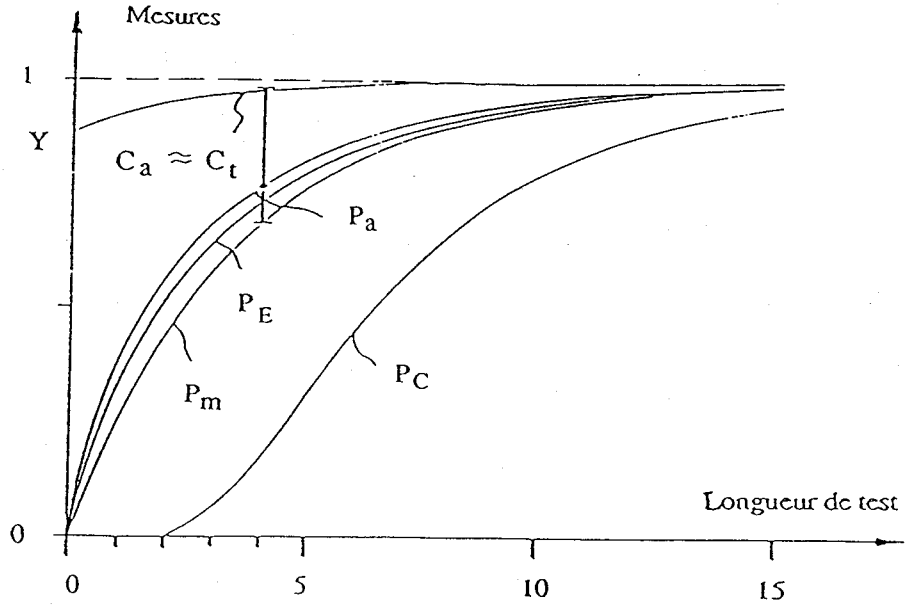


Figure 3.4 : Différentes mesures pour la porte ET à deux entrées

3 . 4 . 2 . Propriétés

Les définitions que nous venons d'énoncer nous permettent d'établir dans le cas général (pour tout circuit, pour toute séquence de test et pour tout ensemble de fautes prescrit) les relations qui lient les différentes notions de la confiance dans la séquence de test.

Propriété 3.4 : Si toutes les fautes sont équiprobables alors la couverture des circuits défectueux est égale à la couverture de fautes espérée.

$$P_a(\Omega_e) = P_E$$

Démonstration : Lorsque les fautes sont équiprobables on a :

$$\Omega = (Pr\,[f_1/F], Pr\,[f_2/F], ..., Pr\,[f_M/F]) = (1/M, ...,1/M) = \Omega_e$$

D'où on peut calculer à partir de l'équation (3.7) :

$$P_a(\Omega_e) = \frac{1}{M} Pr\,[\, Z_1 \neq Z_0\,] + ... + \frac{1}{M} Pr\,[\, Z_M \neq Z_0\,] = P_E$$

□

Dans le cas général il n'existe pas de relation d'ordre entre la couverture des circuits défectueux P_a et la couverture de fautes espérée P_E. Deux exemples simples permettent d'illustrer cette idée. Dans les deux cas il s'agit de tester un circuit dont l'ensemble de fautes prescrit contient deux fautes. Soit $F = \{f_1, f_2\}$.

Exemple 1 : Soit le test aléatoire de ce circuit tel que $Pr\,[Z_1 \neq Z_0] = 0,2$ et $Pr\,[Z_2 \neq Z_0] = 0,99$. La faute f_2 est beaucoup plus facile à tester que la faute f_1.

a) On peut calculer la couverture de fautes espérée :

$$P_E = \frac{0,2 + 0,99}{2} = 0,595$$

b) Pour calculer la couverture des circuits défectueux il faut connaître la probabilité d'occurrence des fautes f_1 et f_2.

i) Supposons que $Pr\,[f_1/F] = 0,9$ et $Pr\,[f_2/F] = 0,1$. Un grand nombre de circuits défectueux (90%) sont affectés de la faute la plus difficile à tester. On peut calculer :

$$P_a = (0,9 \times 0,2) + (0,1 \times 0,99) = 0,279$$

On a alors $\mathbf{P_a < P_E}$.

ii) Supposons que $Pr\,[f_1/F] = 0,5$ et $Pr\,[f_2/F] = 0,5$. Les fautes sont équiprobables. On peut calculer :

$$P_a = (0,5 \times 0,2) + (0,5 \times 0,99) = 0,595$$

On a alors $\mathbf{P_a = P_E}$.

iii) Supposons que Pr $[f_1/F] = 0,1$ et Pr $[f_2/F] = 0,9$. La faute la plus difficile à tester affecte peu de circuits défectueux (10%). On peut calculer :

$$P_a = (0,1 \times 0,2) + (0,9 \times 0,99) = 0,911$$

On a alors $\mathbf{P_a > P_E}$.

Example 2 : Soit le test déterministe de ce circuit tel que la faute f_2 soit testée par S mais pas la faute f_1, i. e., Pr $[Z_1 \neq Z_0] = 0$ et Pr $[Z_2 \neq Z_0] = 1$.

a) On peut calculer la couverture de fautes espérée (dans ce cas *taux de couverture*) :

$$P_E = \frac{0+1}{2} = 0,5$$

b) La couverture des circuits défectueux dépend de la probabilité d'occurrence des fautes f_1 et f_2.

i) Supposons que Pr $[f_1/F] = 0,9$ et Pr $[f_2/F] = 0,1$. On peut calculer :

$$P_a = (0,9 \times 0) + (0,1 \times 1) = 0,1$$

On a alors $\mathbf{P_a < P_E}$.

ii) Supposons que Pr $[f_1/F] = 0,5$ et Pr $[f_2/F] = 0,5$.On peut calculer :

$$P_a = (0,5 \times 0) + (0,5 \times 1) = 0,5$$

On a alors $\mathbf{P_a = P_E}$.

iii) Supposons que Pr $[f_1/F] = 0,1$ et Pr $[f_2/F] = 0,9$.

$$P_a = (0,1 \times 0) + (0,9 \times 1) = 0,9$$

On a alors $\mathbf{P_a > P_E}$.

□

On voit à travers ces deux exemples que si la faute la plus difficile à tester est peu probable alors la couverture de fautes espérée est une mesure pessimiste de la confiance dans la séquence de test par rapport à P_a ($P_E < P_a$). En revanche si la faute la plus difficile à tester est fréquente dans les circuits défectueux P_E est une mesure optimiste par rapport à P_a ($P_E > P_a$). Il me semble important de ne pas risquer de sur-estimer la confiance dans le test. C'est pourquoi je pense que si on ne sait pas au moins majorer la probabilité d'occurrence de la faute la plus difficile à tester il vaut mieux évaluer la confiance dans la séquence de test à partir de la probabilité minimum de test qui est dans tous les cas une estimation pessimiste comme nous allons le voir.

Dans l'exemple du test de la porte ET à deux entrées que nous avons développé on a :

$$P_E = \frac{5}{6}\left(1 - \left(\frac{3}{4}\right)^L\right) + \frac{1}{6}\left(1 - \left(\frac{1}{4}\right)^L\right)$$

$$P_a = 0,75\left(1 - \left(\frac{3}{4}\right)^L\right) + 0,25\left(1 - \left(\frac{1}{4}\right)^L\right)$$

Dans P_a le coefficient 0,25 correspond à Pr [f_6/F] qui est la faute la plus facile à tester (les 5 autres fautes sont toutes les plus difficiles à tester). On peut remarquer que si Pr [f_6/F] > 1/6 alors $P_a > P_E$ et si Pr [f_6/F] < 1/6 alors $P_a < P_E$. La figure 3.5 montre la plage dans laquelle se situe P_a lorsque Pr [f_6/F] varie entre 0 et 1.

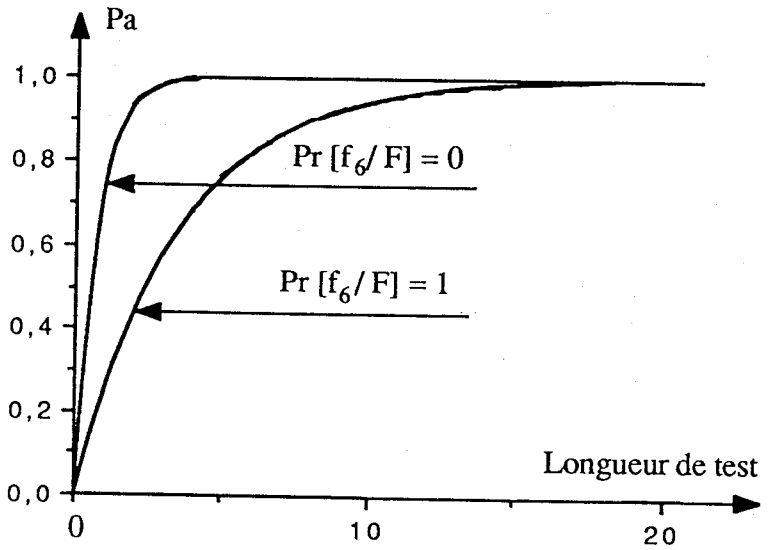


Figure 3.5 : Valeurs possibles de P_a

Théorème 3.2 : Pour tout circuit, pour tout ensemble de fautes et pour toute séquence de test, la couverture des circuits défectueux et la couverture de fautes espérée sont supérieures ou égales à la probabilité minimum de test qui est supérieure ou égale à la probabilité de la couverture complète.

$$P_E \text{ et } P_a \geq P_m \geq P_c$$

Démonstration : Supposons que f_1 soit la faute la plus difficile à tester on a alors :

$$P_m = Pr\,[Z_1 \neq Z_0] \text{ et } Pr[\,Z_i \neq Z_0\,] \geq Pr[\,Z_1 \neq Z_0\,] \quad \text{pour tout } i = 2, \ldots, M.$$

a) $\mathbf{P_E \geq P_m}$: D'après la définition 3.5 on peut écrire :

$$P_E \geq \frac{Pr[Z_1 \neq Z_0] + \ldots + Pr[Z_1 \neq Z_0]}{M} = P_m$$

b) $\mathbf{P_a \geq P_m}$: D'après la définition 3.2 on peut écrire :

$$P_a \geq Pr[\,Z_1 \neq Z_0\,]\,(\,Pr[\,f_1 / F\,] + \ldots + Pr[\,f_M / F\,]\,)$$

On a de plus $Pr[\,f_1 / F\,] + \ldots + Pr[\,f_M / F\,] = 1$ d'où $P_a \geq Pr[\,Z_1 \neq Z_0\,] = P_m$.

c) $\mathbf{P_m \geq P_c}$: A partir de la définition 3.4 on peut écrire :

$$P_c = Pr[\,Z_1 \neq Z_0\,]\,Pr[\,(Z_2 \neq Z_0) \text{ et } (\,Z_3 \neq Z_0) \text{ et } \ldots \text{ et } (Z_M \neq Z_0) / Z_1 \neq Z_0\,]$$

$Pr[(Z_2 \neq Z_0)$ et $(Z_3 \neq Z_0)$ et ... et $(Z_M \neq Z_0) / Z_1 \neq Z_0] \leq 1$ d'où : $P_C \leq Pr[Z_1 \neq Z_0] = P_m$. □

La probabilité de la couverture complète P_c est une *mesure très pessimiste* de la capacité de la séquence de test à détecter un circuit défectueux. La couverture complète des circuits défectueux consiste à tester pour chaque circuit toutes les fautes qui peuvent l'affecter alors qu'une seule d'entre elles est présente. Seule la faute la plus difficile à tester intervient dans la calcul de la probabilité minimum de test P_m. Cette mesure est donc plus grande que P_c. Elle reste néanmoins pessimiste par rapport à P_E et P_a qui tiennent compte du fait qu'un circuit défectueux peut être affecté d'une faute quelquonque de F.

Le théorème 3.2 et la propriété 3.4 permettent de comparer numériquement les différentes mesures de la confiance dans la séquence de test. La confiance dans les circuits testés s'écrit en fonction de la couverture des circuits défectueux P_a qui apparaît donc être la référence. C'est-à-dire qu'elle mesure véritablement la confiance dans la séquence de test alors que les autres mesures sont une estimation de cette confiance.

Toutefois pour être utile une mesure doit pouvoir être calculée assez facilement. Le tableau de la figure 3.6 illustre l'*information nécessaire* au calcul de chaque mesure de la confiance dans la séquence de test pour un circuit combinatoire.

	vecteurs de test pour chaque faute	#de vecteurs de test pour chaque faute	#de vecteurs de test pour la faute la plus difficile à tester	Pr [f_i /F] pour chaque faute	Y rende-ment
P_c	X	X	X		
P_E		X	X		
P_m			X		
P_a		X	X	X	
C_t		X	X	X	X
C_a		X	X	X	X

X : Information nécessaire X : Information implicitement nécessaire

Figure 3.6 : Information nécessaire pour les différentes mesures.

Une croix dans ce tableau signifie que l'information correspondant à cette colonne est nécessaire pour calculer la mesure correspondant à cette ligne. Une croix en pointillés signifie que

l'information de la colonne n'est pas en elle-même utile pour calculer la mesure de la ligne mais que cette information est contenue dans l'information nécessaire. Par exemple il faut connaître le nombre de vecteurs qui testent chaque faute pour calculer P_E. Si ceci est connu alors on connait aussi le nombre de vecteurs qui testent la faute la plus difficile à tester. Pour un circuit séquentiel les informations nécessaires sont plus complexes. Toutefois il existe les mêmes relations de connaissance implicite entre les différentes informations nécessaires. C'est-à-dire que pour tout circuit l'information nécessaire au calcul de P_c implique l'information nécessaire au calcul de P_E qui implique elle-même l'information nécessaire au calcul de P_m.

Soit I (X) l'information nécessaire au calcul de la mesure X. Le tableau de la figure 3.6 permet d'écrire les relations suivantes :

$$I(P_c) \text{ et } I(P_a) \supset I(P_E) \supset I(P_m)$$

L'information nécessaire au calcul de la couverture des circuits défectueux ne peut être comparée à l'information nécessaire au calcul de la probabilité de la couverture complète. En effet la connaissance de tous les vecteurs de test pour chaque faute de F et la connaissance du profil d'occurrence ne sont pas des informations de même nature. La première demande des calculs fastidieux, la seconde suppose une connaissance parfaite de la technologie des circuits testés.

A la figure 3.7 les différentes mesures de la confiance dans la séquence de test sont comparées par rapport à deux critères : la qualité de la mesure, matérialisée par l'axe horizontal, et la difficulté d'obtention, matérialisée par l'axe vertical. La mesure idéale si elle existait se trouverait à l'origine des axes. Lorsqu'une mesure est supérieure ou égale à une autre elle est représentée comme étant supérieure (ce qui est vrai dans le cas général). Un disque signifie que la qualité et la difficulté d'obtention de la mesure correspondante sont exactement connues par rapport à P_a.

Il est clair sur cette figure que :

1) la probabilité de la couverture complète est une mesure de la confiance dans la séquence de test à écarter. Elle est très pessimiste et de plus très difficile à calculer.

2) la position des trois autres mesures P_m, P_E et P_a montre bien que plus une mesure est précise plus elle nécessite d'information.

3) la couverture des fautes espérée P_E pourrait constituer une bonne évaluation de la confiance dans la séquence de test. Mais P_E peut dans certains cas être une mesure optimiste ; P_E ne permet donc pas de dimensionner un dispositif de test qui assure une confiance de test donnée.

4) la probabilité minimum de test P_m est par contre une borne inférieure de la confiance dans la séquence de test facile à estimer.

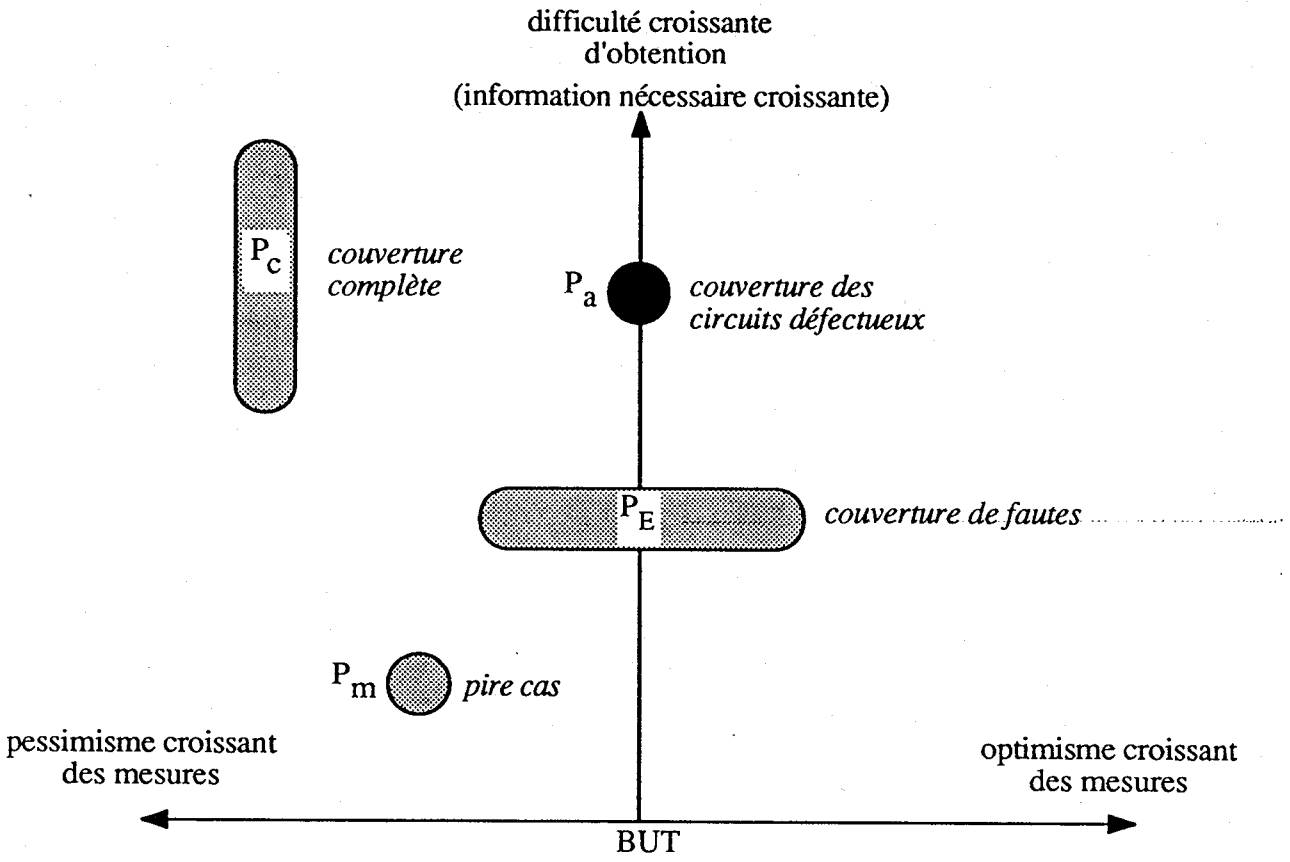


Figure 3.7 : Confiance dans la séquence de test : Comparaison des mesures

Dans le cas particulier du test déterministe que nous allons étudier maintenant les mesures les plus significatives sont mises en évidence.

3 . 5 . Cas particulier : test déterministe

Dans le cas du test déterministe la capacité de la séquence de test à tester une faute est connue exactement. En effet la séquence de test est entièrement connue donc pour chaque faute de F on sait si S permet ou non de la tester. La probabilité de test d'une faute est égale à 1 ou à 0. On peut distinguer deux cas. Soit la séquence de test est un **test complet** pour F, c'est-à-dire que toutes les fautes de F sont testées par S. Soit la séquence de test ne teste pas toutes les fautes de F. Nous proposons de calculer la valeur des six mesures de la confiance dans le test que nous avons définies précédemment pour chacun de ces deux cas.

Propriété 3.5 : Si la séquence de test déterministe S est un test complet pour F, c'est-à-dire :

$$\Pr [Z_i \neq Z_0] = 1 \qquad \forall\, i = 1, \ldots M$$

alors on a :

$$P_c = P_E = P_m = P_a = C_t = C_a = 1$$

Démonstration : Cette propriété s'écrit immédiatement à partir des définitions 3.2 et 3.4 à 3.6 ainsi que des propriétés 3.2 et 3.3.

□

Si la séquence de test assure un test complet de F, c'est-à-dire $P_c = 1$, alors la séquence de test est infaillible. Tous les circuits défectueux sont correctement testés ce qui entraine une confiance totale dans les circuits testés. On a :

$$P_c = 1 \Rightarrow P_E = 1 \text{ et } P_m = 1 \text{ et } P_a = 1$$
$$P_a = 1 \Rightarrow C_t = 1 \text{ et } C_a = 1$$

Remarque 3.6 : Lorsque toutes les fautes sont testées leur probabilité d'occurrence n'intervient pas. On a $P_E = P_a$ même si les fautes ne sont pas équiprobables.

□

Propriété 3.6 : Soit h le nombre de fautes testées par S ($h \neq M$). Supposons que :

$$\Pr[Z_i \neq Z_0] = 1 \quad \forall\, i = 1, \ldots h, \quad \text{et} \quad \Pr[Z_i \neq Z_0] = 0 \quad \forall\, i = h+1, \ldots M$$

On a alors :

$$P_c = 0$$
$$P_E = \frac{h}{M}$$
$$P_m = 0$$
$$P_a = \Pr[f_1/F] + \ldots + \Pr[f_h/F]$$
$$C_t = Y + (1 - Y)\, P_a$$
$$C_a = \frac{Y}{Y + (1 - Y)(1 - P_a)}$$

Démonstration : Cette propriété s'écrit immédiatement à partir des définitions 3.2 et 3.4 à 3.6 ainsi que des propriétés 3.2 et 3.3.

□

Si certaines fautes ne sont pas testées par la séquence de test alors on a $P_c = P_m = 0$ même si une seule faute n'est pas testée. Ces mesures n'ont alors plus vraiment de sens puisque certains circuits défectueux sont malgré tout détectés.

Dans ce cas P_E et P_a sont les deux seules mesures de la confiance dans la séquence de test qui ne soient pas triviales.

La couverture de fautes espérée P_E correspond à la mesure très utilisée qu'est le *taux de*

couverture de fautes.

La couverture des circuits défectueux P_a est une mesure plus fine qui tient compte de la probabilité d'occurrence des fautes testées. Les fautes qui ne sont pas testées ne contribuent pas à la confiance de test.

Par ailleurs on vérifie facilement que dans chacun des deux cas possibles (propriétés 3.5 et 3.6) les relations d'ordre démontrées dans le cas général dans la partie précédente sont vérifiées en particulier pour une séquence de test déterministe.

L'étude comparative des quatre mesures de la confiance dans la séquence de test que nous avons développée jusque là conduit à la conclusion suivante : **P_a est la valeur que l'on veut connaître**. Mais en général il n'est pas possible de calculer la probabilité de test et la probabilité d'occurrence de chaque faute. La mesure **P_m est facile à obtenir** mais entraîne un sur-coût du test du fait de son pessimisme. Nous avons développé une méthode approchée qui permet d'estimer P_a avec une bonne précision à partir de l'étude des seules fautes difficiles à tester, c'est-à-dire des calculs de P_m. La description de cette nouvelle méthode ainsi que ses propriétés font l'objet du chapitre 4.

La définition formelle des six mesures de la confiance dans un test que nous avons donnée dans ce chapitre nous a permis de démontrer certaines propriétés qui les relient. En particulier nous avons montré que la probabilité de la couverture complète est une mesure très pessimiste de la confiance dans la séquence de test et qui de plus est difficile à obtenir. La mesure la plus significative, la couverture des circuits défectueux, est également difficile à obtenir. La probabilité de détecter la faute la plus difficile à tester est une mesure pessimiste de la confiance dans la séquence de test qui est facile à obtenir.

Chapitre 4

Une nouvelle approche d'estimation de la confiance de test

A la lumière des résultats obtenus au chapitre précédent deux mesures sont intéressantes pour estimer la capacité de la séquence de test à détecter un circuit défectueux : la couverture des circuits défectueux qui est la plus significative et la probabilité minimum de test qui est la plus facile à obtenir. A partir de ces deux mesures nous présentons dans ce chapitre une nouvelle approche qui permet d'estimer la mesure la plus significative à l'aide de la plus facile à obtenir calculée sur des sous-ensembles de fautes.

4 . 1 . Introduction

Tout acte commercial commence par la rencontre de deux parties qui ont des intérêts particuliers différents. D'une part le client qui exige une certaine qualité du produit qu'il achète, d'autre part le fournisseur qui essaie de réduire le plus possible le prix de revient de ce qu'il vend. Les circuits digitaux n'échappent pas à cette règle.

Le client, ici *l'utilisateur* des circuits testés, veut accorder une *confiance justifiée* dans les circuits qu'il utilise, c'est pourquoi il exige que le test appliqué aux circuits réponde à un critère de qualité. Par exemple l'utilisateur des circuits testés accepte qu'un circuit sur mille, parmi ceux qui lui ont été livrés, soit défaillant. Le fournisseur, ici *le fabricant* de circuits, met en oeuvre le dispositif de test et veut minimiser le *coût du test* tout en répondant aux exigences de son client.

En termes de confiance de test le fabricant des circuits, afin de garantir la confiance exigée, peut estimer la confiance dans la séquence de test à partir de la probabilité minimum de test. Mais, si cette méthode est très facile à mettre en oeuvre, son application est onéreuse en *temps de test*. Ceci est d'autant plus vrai que le nombre de circuits à tester est grand. L'exemple simple du test aléatoire d'une porte ET à deux entrées permet de l'illustrer. En effet pour cette porte on a :

$$P_m = 1 - \left(\frac{3}{4}\right)^L$$

Si l'exigence de confiance est que un circuit défectueux sur mille passe le test on a :

$$0{,}999 = 1 - \left(\frac{3}{4}\right)^L$$

Soit une longueur de test de $\mathbf{L = 25}$.

La couverture des circuits défectueux permet également de garantir un niveau de confiance. Pour la porte ET à deux entrées on écrira :

$$P_a = 0{,}75\left(1 - \left(\frac{3}{4}\right)^L\right) + 0{,}25\left(1 - \left(\frac{1}{4}\right)^L\right)$$

Le coefficient 0,75 (0,25 respectivement) représente la probabilité d'occurrence d'une faute testée par 1 (3 respectivement) vecteur, cette probabilité est calculée à partir des données de la figure 3.3.

Soit pour $P_a = 0,999$ on trouve une longueur de test de **L = 24.**

Supposons maintenant que la faute la plus facile à tester soit 3 fois plus probable que la faute la plus difficile à tester. On a alors :

$$P_a = 0,25\left(1 - \left(\frac{3}{4}\right)^L\right) + 0,75\left(1 - \left(\frac{1}{4}\right)^L\right)$$

Pour $P_a = 0,999$ on trouve une longueur de test de **L = 20.**

La couverture des circuits défectueux conduit à la *longueur de test optimale*. En effet des deux autres mesures présentées au chapitre précédent

1) la probabilité de la couverture complète est encore plus pessimiste que P_m, c'est-à-dire qu'elle conduit à une longueur de test supérieure à celle obtenue à partir de P_m.

2) la couverture de fautes espérée P_E n'assure pas un niveau de confiance. Dans certains cas elle conduit à une longueur de test telle que plusieurs circuits, en moyenne, parmi mille circuits défectueux passent le test.

Pour le fabricant des circuits testés, le temps consacré au test des circuits comprend le *temps de mise en oeuvre* et *le temps de l'expérience*. En test déterministe la longueur du test est minimale (le temps de l'expérience de test est faible), mais l'analyse du circuit nécessaire au calcul des vecteurs de test peut être longue (le temps de mise en oeuvre est important). En test aléatoire l'analyse du circuit est très réduite, mais la longueur du test est importante. La couverture des circuits défectueux minimise le temps de l'expérience de test mais du fait de l'information nécessaire pour l'obtenir (probabilités de test et d'occurrence de chaque faute) elle est coûteuse à mettre en oeuvre. Shedletsky dans [Shedletsky 77] est arrivé à la conclusion que compte tenu de la quasi impossibilté de calculer P_a le test aléatoire n'est pas recommandé lorsqu'un niveau de confiance est exigé. Pour le fabricant, qui cherche à minimiser le temps global du test (mise en oeuvre + expérience), la nouvelle approche d'estimation de la couverture des circuits défectueux que nous proposons dans ce chapitre permet de trouver un **compromis** entre temps de mise en oeuvre et temps d'expérience. Cette approche rend tout à fait efficace le test aléatoire lorsqu'un niveau de confiance est exigé. L'application de cette approche à un microprocesseur réel (chapitre 7) en est, je pense, une illustration convaicante.

Remarque 4.1 : La différence fondamentale entre un test déterministe et un test aléatoire réside

dans le temps de mise en oeuvre. Pour un test déterministe tous les vecteurs de test appliqués sont préalablement calculés. La rapidité de mise en oeuvre est souvent le critère qui guide le choix d'un test aléatoire. C'est pourquoi les idées que nous avons développées jusque là faisaient référence au test aléatoire. Néanmoins l'approche que nous allons présenter s'applique aussi bien au test déterministe qu'au test aléatoire.

□

La *nouvelle approche* que nous proposons consiste à **partitionner** l'ensemble de fautes prescrit. Dans chaque bloc de la partition une étude de pire cas est faite. C'est-à-dire qu'on calcule la probabilité minimum de test dans chaque bloc. La *probabilité minimum pondérée de test* est alors obtenue en calculant la *moyenne pondérée* des probabilités minimum de test. Les coefficients de pondération sont les probabilités d'occurrence des blocs, c'est-à-dire la probabilité qu'un circuit défectueux soit affecté d'une quelconque faute du bloc considéré. Cette estimation de la confiance dans la séquence de test est toujours pessimiste car elle est basée sur des études de pire cas. De plus elle ne nécessite pas de connaître le profil d'occurrence. En effet seules les probabilités d'occurrence d'ensembles de fautes sont nécessaires. En pratique cette approche permet d'estimer P_a avec une bonne précision grâce à des hypothèses simples .

4 . 2 . Sous-ensembles de F

Les quatre mesures de la confiance dans la séquence de test que nous avons présentées dans le chapitre 3 peuvent être définies sur tout sous-ensemble F_j de F. Dans ce chapitre nous nous intéressons plus particulièrement à la couverture des circuits défectueux et à la probabilité minimum de test qui sont la plus significative et la plus facile à obtenir, respectivement.

Soit $\mathbf{F_j = \{f_1^j, ..., f_{nj}^j\}}$un sous-ensemble de F ($f_k^j \in F, \forall\ k = 1, ..., n_j$). On notera $\mathbf{Z_k^j}$ la réponse d'un circuit lorsque la faute f_k^j est présente. La **probabilité d'occurrence d'un sous-ensemble** $\mathbf{F_j}$ sachant que le circuit est défectueux, notée $\mathbf{Pr\ [F_j / F]}$, est la probabilité qu'un circuit défectueux soit affecté d'une faute qui appartient à F_j. D'après l'hypothèse 3.1 les fautes f_k^j sont exclusives. On peut donc écrire :

$$Pr\ [F_j / F] = Pr\ [f_1^j / F] + ... + Pr\ [f_{nj}^j / F] \qquad (4.1)$$

Exemple 4.1 : Supposons tester une carte composée d'un microprocesseur et d'une mémoire. Soit F l'ensemble des fautes qui peuvent affecter la carte. Soient F_1 et F_2 l'ensemble des fautes qui peuvent affecter le microprocesseur et la mémoire respectivement, $F = \{ F_1, F_2\}$. Soit f_1^1 le collage à 1 de l'indicateur de 0 du microprocesseur. La probabilité $Pr\ [f_1^1 / F_1]$ est la probabilité que

l'indicateur de 0 du microprocesseur soit collé à 1 sachant que le microprocesseur est défectueux. □

A l'aide de ces définitions on peut écrire la relation suivante :

$$Pr [f_k^j / F] = Pr [f_k^j / F_j] \, Pr [F_j / F] \qquad (4.2)$$

Définition 4.1 : Soit $F_j = \{f_1^j, ..., f_{nj}^j\}$ un sous-ensemble de F.

a) La **couverture des circuits défectueux sur F_j** notée $P_a(F_j)$, est la probabilité de détecter un circuit défectueux lorsqu'une faute appartenant à F_j est présente.

$$P_a(F_j) = Pr [Z \neq Z_0 / F_j]$$

b) La **probabilité minimum de test sur F_j** notée $P_m(F_j)$, est la probabilité minimum de détecter un circuit défectueux sachant qu'une faute appartenant à F_j est présente.

$$P_m(F_j) = \min (P_T (f_1^i), ..., P_T (f_{nj}^i))$$

□

Les fautes f_k^j constituent un système complet d'événements sur F_j on peut donc écrire :

$$P_a (F_j) = Pr [Z \neq Z_0 / f_1^j] \, Pr [f_1^j / F_j] + ... + Pr [Z \neq Z_0 / f_{nj}^j] \, Pr [f_{nj}^j / F_j]$$

Soit avec les notations que nous avons définies :

$$P_a (F_j) = Pr [Z_1^j \neq Z_0] \, Pr [f_1^j / F_j] + ... + Pr [Z_{nj}^j \neq Z_0] \, Pr [f_{nj}^j / F_j] \qquad (4.3)$$

Les relations d'ordre qui font l'objet du théorème 3.2 ont été démontrées pour tout ensemble de fautes. Elles sont en particulier vraies sur un sous-ensemble de F. On a donc pour tout sous-ensemble F_j de F :

$$\forall F \supset F_j \quad P_m(F_j) \leq P_a(F_j) \qquad (4.4)$$

Lorsque les sous-ensembles F_j de F constituent une partition de F alors la propriété d'exclusion qui est vraie sur les fautes est vraie aussi sur les sous-ensembles de F. On peut alors faire sur les sous-ensembles de F une étude similaire à celle faite sur les fautes.

4 . 3 . Partitions de F

Une partition ρ de F est un ensemble de sous-ensembles disjoints de F dont l'union constitue F :

$$\rho = \{F_1, ..., F_r\} \text{ avec } F_i \cap F_j = \varnothing, \text{ pour tout } i \neq j, \text{ et } \cup\{F_i\} = F$$

On appelle **un bloc** un élément F_j de la partition. Chaque faute de F appartient à un et un seul sous-ensemble F_j. Les blocs de toute partition de F constituent un *ensemble complet d'événements* sur F. On peut donc écrire pour toute partition $\rho = \{F_1, ..., F_r\}$ de F :

$$Pr [F] = Pr [F_1/F] + ... + Pr [F_r/F] \qquad (4.5)$$

La partition **identité** notée **I** est la partition qui contient un seul bloc : $I = \{F\}$. La partition **zéro** notée **0** est la partition dans laquelle chaque bloc contient une seule faute : $0 = \{\{f_1\}, ..., \{f_M\}\}$. Il existe une relation d'ordre partiel sur l'ensemble des partitions. Soient ρ_1 et ρ_2 deux partitions. On dit que $\rho_1 \leq \rho_2$ si et seulement si chaque bloc de ρ_1 est contenu dans un bloc de ρ_2. En particulier toute partition est comprise entre la partition zéro et la partition identité [Hartmanis 66].

$$\forall \rho, \qquad 0 \leq \rho \leq I \qquad (4.6)$$

Exemple 4.2 : Soit $F = \{f_1, f_2, f_3, f_4\}$ un ensemble de 4 fautes. Il existe 15 partitions sur F. Soient en particulier les 5 partitions suivantes :
$0 = \{\{f_1\}, \{f_2\}, \{f_3\}, \{f_4\}\}$, $\rho_1 = \{\{f_1\}, \{f_2, f_3\}, \{f_4\}\} = \{F_1, F_2, F_3\}$, $\rho_2 = \{\{f_1, f_2\}, \{f_3\}, \{f_4\}\} = \{G_1, G_2, G_3\}$, $\rho_3 = \{\{f_1, f_2, f_3\}, \{f_4\}\} = \{H_1, H_2\}$ et $I = \{f_1, f_2, f_3, f_4\}$.

Les relations d'inclusion qui existent entre ces sous-ensembles sont les suivantes :

1) F_1 et G_1 et $H_1 \supset f_1$, F_2 et G_1 et $H_1 \supset f_2$, F_2 et G_2 et $H_1 \supset f_3$, F_3 et G_3 et $H_2 \supset f_4$

d'où $$0 < \rho_1 \quad \text{et} \quad 0 < \rho_2 \quad \text{et} \quad 0 < \rho_3$$

Pour chacune des 15 partitions ρ possibles de F on peut trouver que pour toute faute f_i il existe un bloc qui la contient. Dans la cas contraire l'union des blocs de ρ ne constituerait pas F.

2) $F \supset F_1$ et F_2 et F_3 et G_1 et G_2 et G_3 et H_1 et H_2

d'où $$\rho_1 < I \quad \text{et} \quad \rho_2 < I \quad \text{et} \quad \rho_3 < I$$

Pour chacune des 15 partitions ρ possibles de F chaque bloc est inclus dans F. Si ce n'était pas le cas l'union des blocs de ρ ne constituerait pas F.

3) $H_1 \supset F_1$ et $H_1 \supset F_2$ et $H_2 \supset F_3$

d'où $$\rho_1 < \rho_3$$

$H_1 \supset G_1$ et $H_1 \supset G_2$ et $H_2 \supset G_3$

d'où $$\rho_2 < \rho_3$$

Mais il n'existe pas de bloc de ρ_2 qui contienne F_2 et inversement il n'existe pas de bloc de ρ_1 qui contienne G_1. Donc ρ_1 et ρ_2 ne sont pas comparables.

□

Grâce à la relation d'ordre partiel qui existe dans l'ensemble des partitions de F nous allons construire une méthode d'estimation de la couverture des circuits défecutueux.

4 . 4 . Nouvelle approche : la probabilité minimum pondérée de test.

Rappelons en quelques mots le problème à résoudre. La confiance dans les circuits testés dépend de la confiance dans la séquence de test. La mesure de la confiance de test P_a est difficile à obtenir. Il s'agit donc de trouver une méthode qui permette d'estimer P_a à partir d'une information réduite. La difficulté d'obtention de P_a provient du fait qu'il faut étudier chaque faute de F. L'idée de base de l'approche proposée ici est de découper l'ensemble de fautes en plusieurs sous-ensembles et de n'étudier qu'une faute dans chaque sous-ensemble. Le théorème 4.1 permet de comprendre la nécessité d'une telle démarche.

Théorème 4.1 : Pour tout circuit, pour toute séquence de test, pour tout ensemble de fautes F et pour toute partition $\rho = \{F_1, ..., F_r\}$ de F :

a) la couverture des circuits défectueux sur F est la *moyenne* des couvertures des circuits défectueux sur les blocs F_j, pondérée par les probabilités d'occurrence de ces blocs.

$$P_a = Pr\,[F_1/F]\; P_a(F_1) + \ ...+ Pr\,[F_r/F]\; P_a(F_r) \qquad (4.7)$$

b) la probabilité minimum de test est le *minimum* sur ρ des probabilités minimum de test.

$$P_m = \min\,(\,P_m(F_1), ..., P_m(F_r)\,) \qquad (4.8)$$

Démonstration : Afin d'alléger les notations nous allons écrire la démonstration pour r = 2 et $F_1 = \{\ f_1, \ldots, f_h\ \}$, $F_2 = \{\ f_{h+1}, \ldots, f_M\ \}$.

a) D'après l'équation 4.3 on peut écrire :

$$P_a(F_1) = Pr\,[f_1 / F_1]\; P_T(f_1) + ... + Pr\,[f_h / F_1]\; P_T(f_h) \qquad (4.9)$$

$$P_a(F_2) = Pr\,[f_{h+1} / F_2]\; P_T(f_{h+1}) + ... + Pr\,[f_M / F_2]\; P_T(f_M) \qquad (4.10)$$

et d'après l'équation 3.8 :

$$P_a = Pr\,[f_1 / F]\; P_T(f_1) + ... + Pr\,[f_M / F]\; P_T(f_M) \qquad (4.11)$$

En utilisant l'équation (3.1) pour chaque faute $f_i \in F_k$ les équations (4.9 à 4.11) deviennent :

$$P_a(F_1) = \frac{Pr\,[f_1]}{Pr\,[F_1]}\, P_T(f_1) + ... + \frac{Pr\,[f_h]}{Pr\,[F_1]}\, P_T(f_h) \qquad (4.12)$$

$$P_a(F_2) = \frac{Pr\,[f_{h+1}]}{Pr\,[F_1]}\, P_T(f_{h+1}) + ... + \frac{Pr\,[f_M]}{Pr\,[F_1]}\, P_T(f_M) \qquad (4.13)$$

$$P_a = \frac{Pr\,[f_1]}{Pr\,[F]} P_T\,(f_1) + \ldots + \frac{Pr\,[f_M]}{Pr\,[F]} P_T\,(f_M) \qquad (4.14)$$

A partir des équations (4.12 à 4.14) on peut écrire :

$$Pr\,[F]\,P_a = Pr\,[F_1]\,P_a\,(F_1) + Pr\,[F_2]\,P_a(F_2) \qquad (4.15)$$

Si le circuit est défectueux on a Pr [F] = 1 d'où :

$$Pr\,[F_1] = Pr\,[F_1 / F] \text{ et } Pr\,[F_2] = Pr[F_2 / F]$$

et l'équation (4.15) devient :

$$P_a = Pr\,[F_1 / F]\,P_a(F_1) + Pr\,[F_2 / F]\,P_a(F_2)$$

b) Supposons que la faute la plus difficile à tester appartienne à F_1. On a alors :

$$P_m = P_m(F_1) \text{ et } P_m(F_2) \geq P_m(F_1).$$

□

Ce théorème montre que la confiance globale dans la séquence de test peut être obtenue en faisant un ensemble d'études locales sur des sous-ensembles de F. Cependant bien que l'équation (4.7) ne fasse apparaître que des grandeurs relatives aux sous-ensembles F_j de F et pas aux fautes elles-même, cette équation est une nouvelle écriture pour P_a qui nécessite la même information que l'équation (3.8) pour être calculée. En effet on a :

$$P_a\,(F_i) = Pr\,[Z_1^j \neq Z_0]\,Pr\,[\,f_1^j / F_i] + \ldots + Pr\,[Z_{nj}^j \neq Z_0]\,Pr\,[\,f_{nj}^j / F_j]$$

avec

$$Pr\,[f_1^j/F_j] = \frac{Pr\,[f_1^j/F]}{Pr\,[F_j/F]}$$

donc la probabilité de test et la probabilité d'occurrence de chaque faute sont nécessaires. Par contre les coefficients de pondération Pr [F_j/F] représentent la fonction de distribution des sous-ensembles F_j. Ils peuvent être calculés sans nécessairement connaître la distribution des fautes de F_j. Seule la somme des probabilités d'occurrence des fautes appartenant à F_j est nécessaire (équation (4.1)), non pas chaque probabilité qui la compose.

Ce théorème met en évidence la fait que l'information nécessaire est presque intégralement contenue dans la mesure de la confiance sur chaque bloc. Nous proposons d'utiliser sur chaque bloc une mesure de confiance facile à obtenir, à savoir la probabilité minimum de test.

Définition 4.2 : Soit ρ une partition de F, ρ = {F_1, ... , F_r}. La **probabilité minimum pondérée de test** sur F relative à ρ notée $\mathbf{P_w}$ (ρ), est la moyenne pondérée des probabilités minimum de test sur chaque bloc de ρ.

$$P_w\,(\rho) = Pr\,[F_1/F]\,P_m(F_1) + \ldots + Pr\,[F_r/F]\,P_m(F_r)$$

□

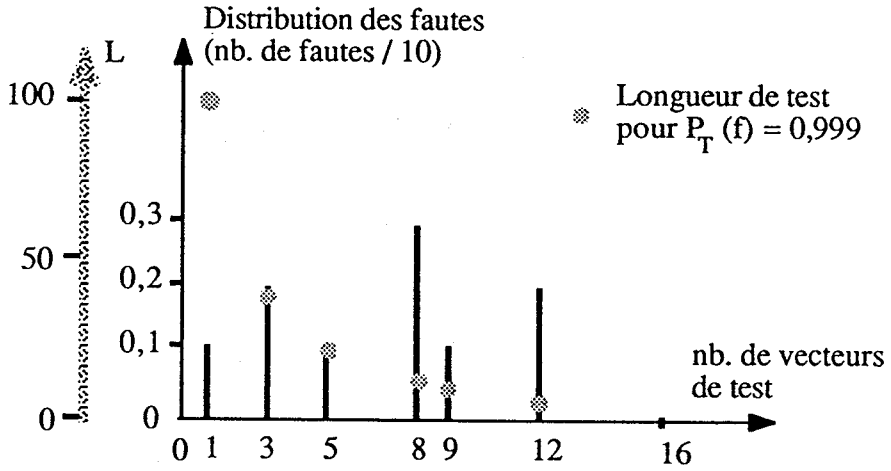
Un exemple simple nous permettra d'illustrer cette définition.

Exemple 4.3 : Soit le test d'un circuit combinatoire fictif à 4 entrées dont l'ensemble de fautes

prescrit comprend 10 fautes, F = $\{f_1, ..., f_{10}\}$, qui sont supposées équiprobables. Le nombre de vecteurs d'entrée qui testent chaque faute est donné dans la tableau de la figure 4.1a. L'information contenue dans ce tableau est représentée sous forme de graphique à la figure 4.1b. Ce graphe représente le profil de détection utilisé dans [Wagner 87] et [Malayia 84], c'est-à-dire le nombre de fautes de F testées par un même nombre de vecteurs d'entrée. Par exemple 8 vecteurs d'entrée parmi les 16 possibles permettent de tester la faute f_6 et il existe 3 fautes de F qui sont testées par 8 vecteurs d'entrée (f_4, f_6, f_7).

fautes	f1	f2	f3	f4	f5	f6	f7	f8	f9	f10
nombre de vecteurs de test	1	3	3	8	5	8	8	9	12	12

- a -



- b -

Figure 4.1 : Exemple d'un ensemble fictif de fautes
a - Fautes prescrites b - Distribution des fautes

Pour un circuit combinatoire le nombre de vecteurs qui testent une faute f_i est une image de la probabilité de test par un vecteur de cette faute. Si les fautes sont équiprobables le nombre de fautes testées par k vecteurs caractérise la probabilité d'occurrence d'une faute testée par k vecteurs d'entrée. La longueur de test qui réalise $P_T(f_i) = 0,999$ est également représentée sur le graphe de la figure 4.1b. Pour donner une image on peut dire que la longueur de test qui assure $P_a = 0,999$ est la moyenne des 6 longueurs de test obtenues en calculant $P_T(f_i) = 0,999$ pour les 10 fautes de F, pondérée par le nombre moyen de fautes qui conduisent à cette longueur de test.

A partir des données du tableau de la figure 4.1a on peut calculer :

$$P_a = P_E = \frac{1}{10}\left(\left(1-\left(1-\frac{1}{16}\right)^L\right)+2\left(1-\left(1-\frac{3}{16}\right)^L\right)+\left(1-\left(1-\frac{5}{16}\right)^L\right)+3\left(1-\left(1-\frac{8}{16}\right)^L\right)+\left(1-\left(1-\frac{9}{16}\right)^L\right)+2\left(1-\left(1-\frac{12}{16}\right)^L\right)\right)$$

Pour $P_a \geq 0{,}999$ on calcule une longueur de test de **L = 72.**

Soit $\rho_1 = \{F_1, F_2\}$ une partition de F avec

$$F_1 = \{f_1, f_2, f_3, f_4\} \text{ et } F_2 = \{f_5, f_6, f_7, f_8, f_9, f_{10}\}$$

Les fautes appartenant à F_1 sont représentées en traits pleins à la figure 4.2a et les fautes appartenant à F_2 sont représentées en traits gris.

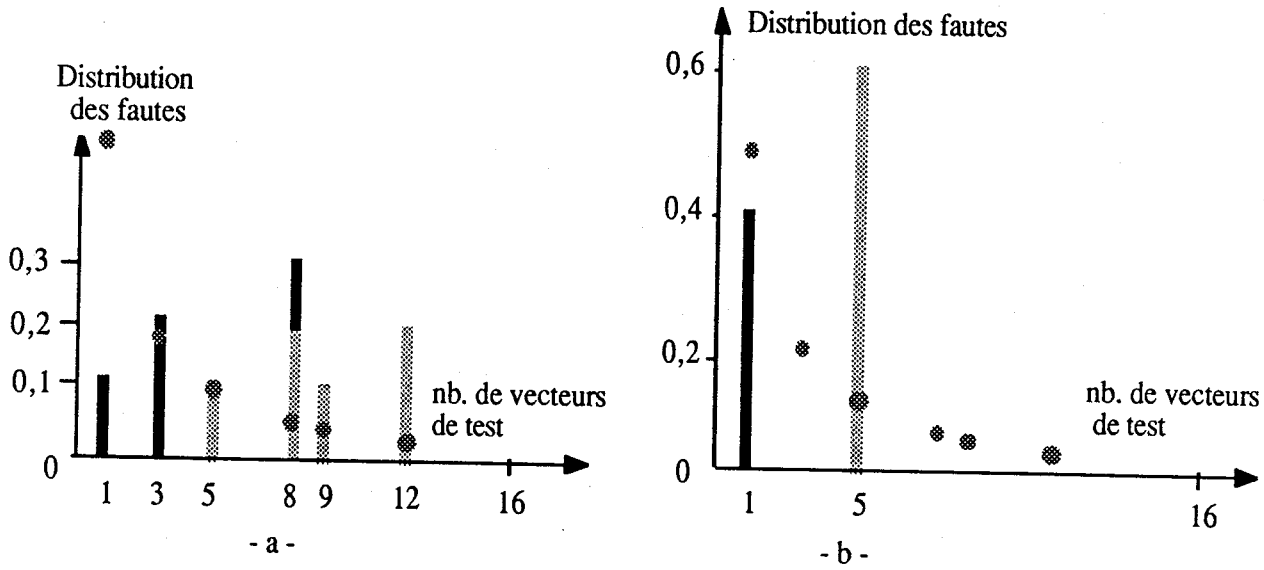


Figure 4.2 : Exemple fictif de 10 fautes
a - Distribution des fautes b - Distribution des blocs de la partition ρ_1

Le calcul de $P_w(\rho_1)$ consiste à affecter à toutes les fautes de F_1 (resp. F_2) la probabilité de test de la faute la plus difficile à tester dans F_1 (resp. F_2). La confiance dans la séquence de test est alors obtenue à partir du profil de détection représenté à la figure 4.2b. Tout se passe comme si on n'avait que deux fautes possibles, l'une testée par un seul vecteur d'entrée, l'autre testée par 5 vecteurs d'entrée. La probabilité d'occurrence de la première est égale à 0,4 (F_1 contient 4 fautes), celle de la seconde à 0,6 (F_2 contient 6 fautes). On peut donc calculer :

$$P_w(\rho_1) = Pr[F_1/F]\, P_m(F_1) + Pr[F_2/F]\, P_m(F_2)$$

$$P_w(\rho_1) = 0{,}4\left(1-\left(1-\frac{1}{16}\right)^L\right)+0{,}6\left(1-\left(1-\frac{5}{16}\right)^L\right) \qquad (4.16)$$

Pour $P_w(\rho_1) = 0{,}999$ on trouve **L = 93** (ce résultat est arrondi, l'équation (4.16) conduit à L = 92,835 479 36).

□

Savir et Bardell dans [Savir 84] utilisent ce genre d'approximation pour estimer la probabilité de la couverture complète. En effet ils font l'hypothèse que toutes les fautes qui ont une probabilité de test inférieure au double de la probabilité de test de la faute la plus difficile ont une probabilité de test égale à la probabilité de test de la faute la plus difficile. Les autres fautes n'ont pas d'effet sur la longueur de test.

Le tableau de la figure 4.3 illustre l'information nécessaire pour calculer $P_w(\rho)$ pour un circuit combinatoire.

	Prob. de détection de chaque faute	Prob. de détecter la faute la plus difficile à détecter de chaque bloc F_i	Prob. de détecter la faute la plus difficile à détecter	Pr [f_i / F]	Pr [F_i / F]
P_a	X	X	X	X	X
P_m			X		
$P_w(\rho)$		X	X		X

X Information nécessaire X Information implicitement connue

Figure 4.3 : Information nécessaire au calcul de la probabilité minimum pondérée de test

Soit I (X) l'information nécessaire pour obtenir la variable X. On a :

$$\forall \rho \qquad I(P_a) \supset I(P_w(\rho)) \supset I(P_m)$$

Pour calculer $P_w(\rho)$ il faut connaître la probabilité de tester la faute la plus difficile à tester de chaque bloc, et la probabilité qu'un circuit défectueux soit affecté d'une faute appartenant à chacun des blocs de ρ. Nous verrons que d'une part des hypothèses simples permettent d'estimer la probabilité d'occurrence d'un bloc de ρ, et d'autre part pour les ensembles de fautes faciles à tester il suffit de minorer la probabilité minimum de test.

4 . 4 . 1 . Influence de la partition

Théorème 4.2 : Pour tout circuit, pour toute séquence de test, pour tout ensemble de fautes F et pour toutes partitions ρ_1 et ρ_2 de F on a :

a) si $\rho_1 \leq \rho_2$ alors $P_w(\rho_1) \geq P_w(\rho_2)$

b) $P_w(0) = P_a$

c) $P_w(I) = P_m$

Exemple 4.4 : Nous proposons d'illustrer ce théorème par un exemple de 4 fautes avant de le démontrer de façon formelle.

Soient $F = \{f_1, f_2, f_3, f_4\}$ un ensemble de fautes et les partitions suivantes définies sur F :

$$\rho_1 = \{\{ f_1 \}, \{ f_2, f_3 \}, \{ f_4\} \} = \{F_1, F_2, F_3\} \text{ et } \rho_2 = \{\{f_1, f_2, f_3 \}, \{f_4\} \} = \{G_1, G_2\}$$

On a :

$$\rho_1 \leq \rho_2$$

On peut calculer les probabilités d'occurrence de chaque bloc de ρ_1 et de ρ_2 (Eq.(4.1)):

$\Pr [F_1 / F] = \Pr [f_1 / F]$,

$\Pr [F_2 / F] = \Pr [f_2 / F] + \Pr [f_3 / F]$,

$\Pr [F_3 / F] = \Pr [f_4 / F]$,

$\Pr [G_1 / F] = \Pr [f_1 / F] + \Pr [f_2 / F] + \Pr [f_3 / F]$,

$\Pr [G_2 / F] = \Pr [f_4 / F]$.

Soit : $H_1 = \{F_1, F_2\}$

On a $$\Pr [H_1 / F] = \Pr [F_1 / F] + \Pr [F_2 / F] = \Pr [G_1/F] \quad (4.17)$$

D'après les définitions 4.1 et 4.2 on a :

$$P_w(\rho_1) = \Pr [F_1 / F]\, P_T(f_1) + \Pr [F_2 / F] \min (P_T(f_2), P_T(f_3)) + \Pr [F_3 / F]\, P_T(f_4) \quad (4.18)$$

$$P_w(\rho_2) = \Pr [G_1 / F] \min (P_T(f_1), P_T(f_2), P_T(f_3)) + \Pr [G_2 / F]\, P_T(f_4) \quad (4.19)$$

D'après l'équation (4.18) on a :

$$P_w(\rho_1) \geq \Pr [F_1 / F] \min (P_T(f_1), P_T(f_2), P_T(f_3)) + \Pr [F_2 / F] \min (P_T(f_1), P_T(f_2), P_T(f_3)) + \Pr[F_3 / F]\, P_T(f_4) \quad (4.20)$$

D'après les équations (4.17) et (4.20) on a :

$$P_w(\rho_1) \geq \Pr [H_1 / F] \min (P_T(f_1), P_T(f_2), P_T(f_3)) + \Pr [F_3 / F]\, P_T(f_4) \quad (4.21)$$

A partir des équations (4.17), (4.19) et (4.21) on obtient :

$$P_w(\rho_1) \geq P_w(\rho_2)$$

□

Démonstration :

a) Soit $\rho_1 = \{ F_1, \ldots, F_{n1} \}$ et $\rho_2 = \{ G_1, \ldots, G_{n2} \}$ deux partitions de F telles que $\rho_1 \leq \rho_2$ c'est-à-dire que $\forall\, i = 1, \ldots, n1$, $\exists\, j \in \{1, \ldots, n2\}$ tel que $G_j \supset F_i$

On a donc $$P_m(G_j) \leq P_m(F_i). \quad (4.22)$$

Soit H_j l'ensemble des blocs de ρ_1 qui sont contenus dans G_j c'est-à-dire

$$H_j = \{ F_i / G_j \supset F_i \}$$

On peut alors calculer Pr [H_j / F] :

$$\Pr [H_j / F] = \Sigma_i \Pr [F_i / F] \quad \text{pour tout i tel que } G_j \supset F_i \tag{4.23}$$

ρ_1 est une partition de F on a donc $F_i \cap F_k = \varnothing$ pour tout $i \neq k$. D'où :

$$\Pr [H_j / F] = \Pr [G_j / F]. \tag{4.24}$$

Les équations (4.22) à (4.24) nous permettent d'écrire :

$$P_w (\rho_1) = \Pr [F_1 / F] P_m(F_1) + ... + \Pr[F_{n1} / F] P_m(F_{n1})$$
$$\geq \Pr [H_1 / F] P_m(G_1) + ... + \Pr [H_{n2} / F] P_m(G_{n2})$$
$$\geq \Pr [G_1 / F] P_m(G_1) + ... + \Pr [G_{n2} / F] P_m(G_{n2}) = P_w(\rho_2)$$

b) D'après la définition 4.2 on a :

$$P_w (0) = \Pr [f_1 / F] P_T (f_1) + ... + \Pr [f_M / F] P_T (f_M) = P_a \tag{Def . 3.2}$$

c) De même on a :

$$P_w (I) = \Pr [F / F] \min (P_T (f_1), ... , P_T (f_M)) = P_m \tag{Def . 3.6}$$

□

Corollaire 4.1 : Pour tout circuit, pour toute séquence de test, pour tout ensemble de fautes F et pour toute partition ρ de F on a :

$$P_m \leq P_w (\rho) \leq P_a$$

Démonstration : Ce corollaire se déduit immédiatement du théorème 4.2 d'après la relation (4.6).

□

Le corollaire 4.1 et le théorème 4.2 montrent que plus on fait un découpage fin du circuit meilleure est l'estimation de la confiance. On étudie en fait un plus grand nombre de fautes. L'exemple 4.5 illustre ce phénomène.

Exemple 4.5 : A partir de l'ensemble de fautes de l'exemple 4.3 on peut définir la partition ρ_2 suivante :

$$\rho_2 = \{G_1, G_2, G_3\}$$

avec $$G_1 = \{f_1, f_2, f_3\} \text{ et } G_2 = \{f_4\} \text{ et } G_3 = \{f_5, f_6, f_7, f_8, f_9, f_{10}\}$$

On vérifie que $\rho_1 \geq \rho_2$. La figure 4.4 montre la distribution des fautes dans chaque bloc de ρ_2 ainsi que la distribution construite pour calculer $P_w (\rho_2)$.

On peut calculer :

$$P_w (\rho_2) = \Pr [G_1 / F] P_m (G_1) + \Pr [G_2 / F] P_m (G_2) + \Pr [G_3 / F] P_m (G_3)$$

$$P_w (\rho_2) = 0{,}3 \left(1 - \left(1 - \frac{1}{16} \right)^L \right) + 0{,}6 \left(1 - \left(1 - \frac{5}{16} \right)^L \right) + 0{,}1 \left(1 - \left(1 - \frac{8}{16} \right)^L \right) \tag{4.25}$$

Pour $P_w(\rho_2) = 0{,}999$ on trouve **L = 89** (l'équation (4.25) conduit à L = 88,377 954 35).

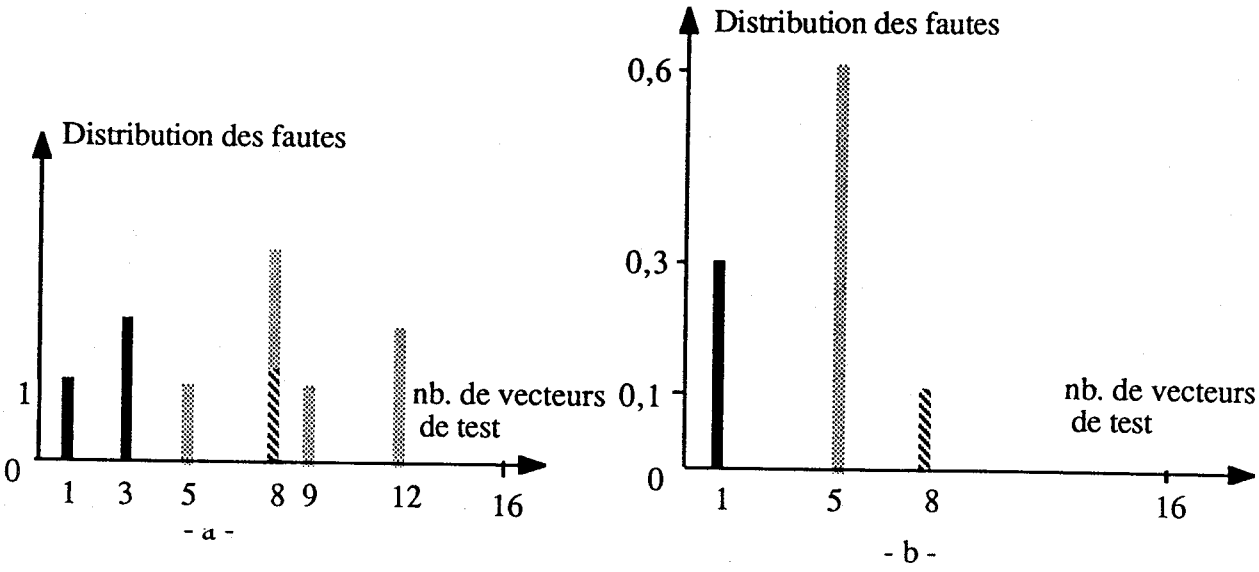


Figure 4.4 : Exemple fictif de 10 fautes
a - Distribution des fautes b - Distribution correspondante à la partition ρ_2

Réciproquement pour **L = 93** on trouve $\mathbf{P_w(\rho_2) = 0{,}99926}$. On vérifie donc que $P_w(\rho_1) \leq P_w(\rho_2)$.

□

Un découpage plus fin de l'ensemble de fautes va bien entendu de pair avec une connaissance plus précise du circuit. Pour l'exemple que nous avons étudié le calcul de $P_w(\rho_1)$ nécessite de connaître (ou d'estimer) les 4 probabilités suivantes :

1) $Pr[F_1 / F] = Pr[f_1 / F] + Pr[f_2 / F] + Pr[f_3 / F] + Pr[f_4 / F]$
2) $Pr[F_2 / F] = Pr[f_5 / F] + Pr[f_6 / F] + Pr[f_7 / F] + Pr[f_8 / F] + Pr[f_9 / F] + Pr[f_{10} / F]$
3) $P_T(f_1)$
4) $P_T(f_5)$

Pour $P_w(\rho_2)$ il faut connaître les 6 probabilités suivantes :

1) $Pr[G_1 / F] = Pr[f_1 / F] + Pr[f_2 / F] + Pr[f_3 / F]$
2) $Pr[G_2 / F] = Pr[f_4 / F]$
3) $Pr[G_3 / F] = Pr[f_5 / F] + Pr[f_6 / F] + Pr[f_7 / F] + Pr[f_8 / F] + Pr[f_9 / F] + Pr[f_{10} / F]$
4) $P_T(f_1)$
5) $P_T(f_4)$
6) $P_T(f_5)$

Pour passer de la partition ρ_1 à la partition plus fine ρ_2 il faut tout connaître sur la faute

f_4 : P_T (f_4) et Pr [f_4 / F] (ou Pr [f_1 / F] + Pr [f_2 / F] + Pr [f_3 / F])

La figure 4.5 présente une synthèse graphique de ces différents commentaires. Le rectangle hachuré représente la région du plan qui contient toutes les estimations P_w (ρ) de P_a.

La probabilité minimum de test P_m correspond à la partition la plus grossière de F puisque $P_m = P_w$ (I). Lorsque l'on affine progressivement la partition on se déplace de P_m vers P_a sur une courbe du type de celles représentées à la figure 4.5. Cette figure met en évidence le problème du choix de la partition. En effet on voit que pour un niveau de connaissance donné la courbe I donne une estimation plus précise que la courbe II. En pratique le choix de la partition optimale ne se pose pas car l'utilisateur de cette méthode va décomposer l'ensemble de fautes prescrit par rapport à des informations dont il dispose ou bien qu'il estime pouvoir avoir facilement. Il s'engagera naturellement sur une courbe de type I.

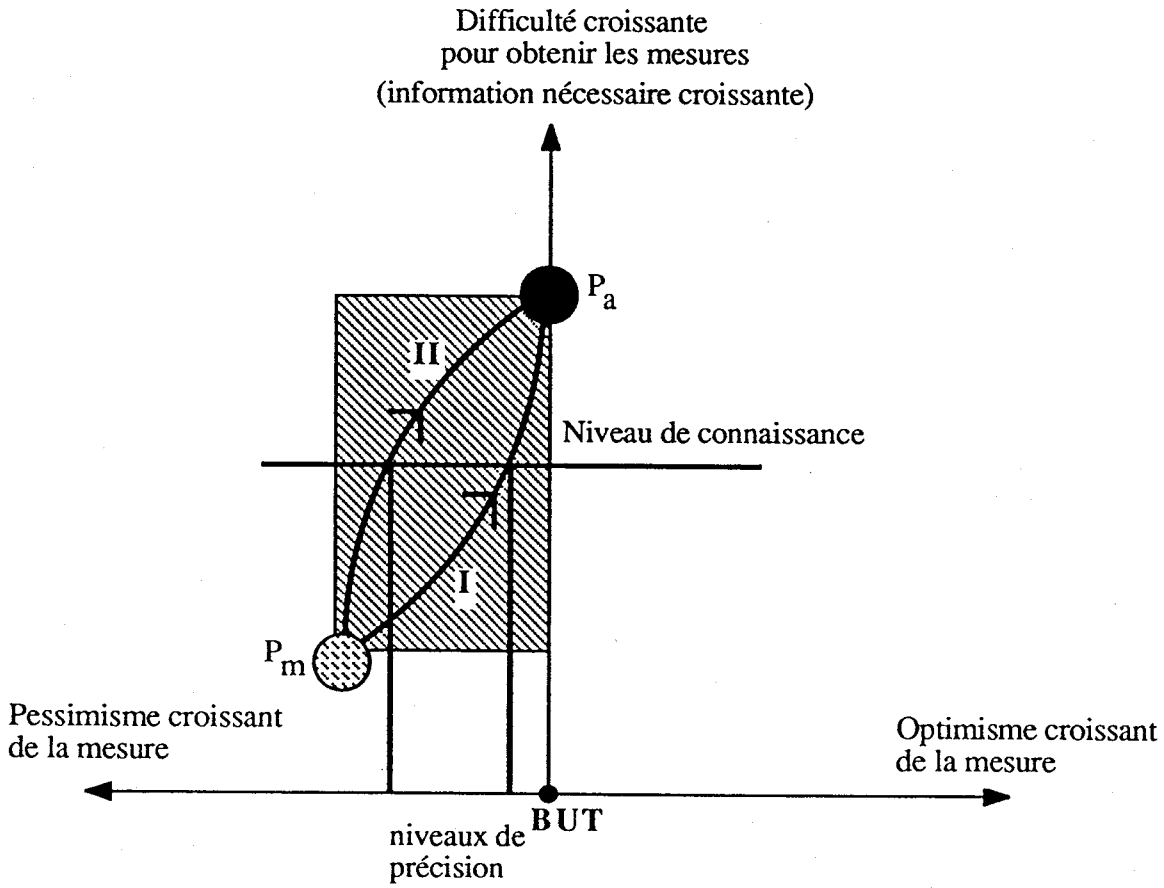


Figure 4.5 : Domaine des estimations possibles
Evolution de P_m vers P_a

4 . 4 . 2 . Choix de la partition

Deux critères permettent de différencier les fautes qui affectent un circuit : la localisation d'une faute et la nature d'une faute.

a - Localisation

La localisation consiste à différencier les fautes par rapport aux éléments qu'elles affectent. Pour un circuit complexe comme un microprocesseur dans lequel on peut distinguer des blocs fonctionnels on pourra dans un premier temps découper l'ensemble de fautes suivant les blocs du circuit.

Exemple 4.6 : Soit le test aléatoire d'une carte qui comprend 4 composants notés I, II, III et IV. Soit F_I, F_{II}, F_{III} et F_{IV} l'ensemble des fautes qui peuvent affecter les composants I, II, III et IV respectivement. On a $F = F_I \cup F_{II} \cup F_{III} \cup F_{IV}$. Une étude de pire cas a été développée pour calculer la longueur du test à appliquer. Pour trouver le composant le plus difficile à tester, c'est-à-dire celui qui peut être affecté de la faute la plus difficile à tester, une étude de pire cas a dû être menée pour chacun des 4 composants. Les résultats sont les suivants :

$$P_m(F_I) = 10^{-3}$$
$$P_m(F_{II}) = 10 \cdot 10^{-3}$$
$$P_m(F_{III}) = 30 \cdot 10^{-3}$$
$$P_m(F_{IV}) = 100 \cdot 10^{-3}$$

Soit $\rho_1 = \{F_I, F_{II}, F_{III}, F_{IV}\}$. Supposons que les quatre composants ont la même probabilité d'être défectueux. On peut alors calculer :

$$P_w(\rho_1) = Pr[F_I/F]\, P_m(F_I) + Pr[F_{II}/F]\, P_m(F_{II}) + Pr[F_{III}/F]\, P_m(F_{III}) + Pr[F_{IV}/F]\, P_m(F_{IV})$$
$$P_w(\rho_1) = 0{,}25\,(1 - (1 - 10^{-3})^L) + 0{,}25\,(1 - (1 - 10 \cdot 10^{-3})^L)$$
$$+ 0{,}25\,(1 - (1 - 30 \cdot 10^{-3})^L) + 0{,}25\,(1 - (1 - 100 \cdot 10^{-3})^L)$$

La probabilité minimum pondérée de test $P_w(\rho)$ permet d'estimer la confiance dans la séquence de test sans étude supplémentaire du circuit. Grâce à cette méthode le fabricant profite de toute l'information dont il dispose.

□

Les nombreux résultats qui existent sur l'analyse des circuits combinatoires permettent également de différencier les fautes. Par exemple on sait que plus un circuit est profond, c'est-à-dire plus il y a de portes logiques sur les chemins qui vont des entrées primaires aux sorties

observables, plus le circuit est difficile à tester. Les résultats sur les *points de contrôle* [Breuer 76], en particulier, permettent de différencier les fautes dans un même circuit par rapport à leur distance aux entrées primaires. L'exemple d'application traité dans la partie 4.5 illustre ce type de démarche.

b - Nature de la faute :

Lorsque l'on a utilisé toutes les informations qui peuvent nous permettre de localiser précisément les fautes on peut les différencier par leur nature. Plusieurs fautes peuvent affecter un même élément, par exemple un collage ou un court-circuit. Là encore de nombreux résultats existent pour les circuits combinatoires. On sait par exemple qu'un collage multiple est plus facile à tester qu'un collage simple. Ce type de critère est utilisé pour différencier les fautes dans le microprocesseur à test intégré (MTI) étudié au chapitre 7.

Ces deux critères guident l'utilisateur de cette méthode dans le choix d'une partition. De plus les différents résultats sur lesquels ils s'appuient permettent le plus souvent de calculer la probabilité minimum pondérée de test correspondante sans que l'utilisateur ait à calculer de nouvelles probabilités de test. En effet dans le paragraphe suivant on montre que pour les fautes qui ne sont pas difficiles à tester, un minorant de la probabilité de test suffit à estimer précisément la confiance dans le séquence de test.

4 . 4 . 3 . Influence de la probabilité de test

En dessous d'un certain niveau de précision on peut, d'un point de vue pratique, ne considérer qu'une partition très grossière des fautes en distinguant d'une part les fautes les plus difficiles à tester et d'autre part les fautes plus faciles à tester. L'exemple de la carte à 4 composants permet d'illustrer cette idée.

Exemple 4.8 : Soit le test de la carte définie dans l'exemple 4.6. La figure 4.6a représente la distribution des fautes par rapport au composant qu'elles affectent. C'est aussi la distribution des fautes associée à la partition ρ_1 définie dans l'exemple 4.6. Pour cette partition on peut calculer la longueur de test qui assure $P_w(\rho_1) = 0{,}999$; on trouve $L = 5\,519$. La figure 4.6b représente la distribution des fautes correspondant à la partition ρ_2 suivante :

$$\rho_2 = \{F_1, F_2\} \quad \text{avec} \quad F_1 = F_I \quad \text{et} \quad F_2 = F_{II} \cup F_{III} \cup F_{IV}$$

Pour cette partition on peut calculer :

$$P_w(\rho_2) = 0{,}25\,(1 - (1 - 10^{-3})^L) + 0{,}75\,(1 - (1 - 10\,10^{-3})^L)$$

Pour $P_w(\rho_2) = 0{,}999$ on trouve **L = 5 519.**

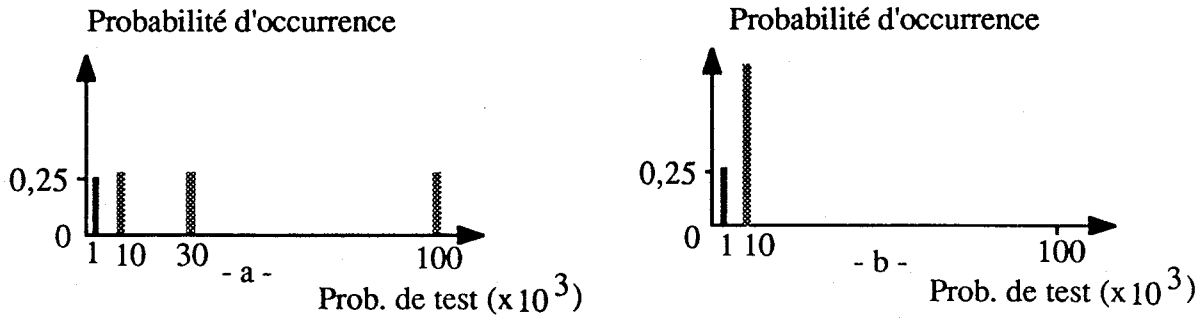


Figure 4.6 : Distribution des fautes
a - Distribution des blocs de ρ_1 b - Distribution des blocs de ρ_2

Ces deux partitions conduisent à la même longueur de test. Pour L = 5 519 on a

$$(1 - 10^{-3})^L = 8{,}14\ 10^{-25}$$

donc *a fortiori* les sous-circuits plus faciles à tester que le sous-circuit II ont une contribution négligeable à la longueur de test. Si on peut montrer que les circuits III et IV sont au moins aussi faciles à tester que le circuit II alors il n'est pas nécessaire de trouver la probabilité de test de la faute la plus difficile à tester de ces deux circuits.

□

L'exemple précédent montre que la probabilité de test des fautes les plus faciles à tester n'est pas un paramètre qui détermine la confiance dans la séquence de test. Il suffit d'en connaître un minorant qui soit assez grand devant P_m. Dans un premier temps on peut donc étudier des partitions du type $\rho = \{F_1, F_2\}$ avec F_1 les fautes les plus difficiles à tester et F_2 les fautes plus faciles à tester. La limite entre fautes difficiles à tester et fautes plus faciles à tester dépend de l'exemple, de la longueur de test obtenue et du compromis entre précision et coût d'analyse que l'on se fixe. La progression de P_m vers P_a (figure 4.5) avec des partitions en deux blocs de ce type consiste à identifier le mieux possible les fautes réellement difficiles à tester. A partir d'un ensemble F_1 de fautes réputées difficiles à tester on peut appliquer différents critères de choix d'une partition pour montrer que certaines de ces fautes sont en réalité faciles à tester.

Exemple 4.9 : Pour l'ensemble de 10 fautes décrit dans l'exemple 4.3 si on peut montrer que f_4 est au moins aussi facile à tester que f_5 alors on définira la partition $\rho_3 = \{F_1, F_2\}$ avec $F_1 = \{f_1, f_2, f_3\}$ et $F_2 = \{f_4, f_5, f_6, f_7, f_8, f_9, f_{10}\}$. On voit bien sur la figure 4.7 que l'approximation faite sur la probabilité de test de la faute f_4 est moins importante dans $P_w(\rho_3)$ que dans $P_w(\rho_1)$.

On a :

$$P_w(\rho_1) = 0{,}4\left(1-\left(1-\frac{1}{16}\right)^L\right)+0{,}6\left(1-\left(1-\frac{5}{16}\right)^L\right) \quad (4.16)$$

$$P_w(\rho_3) = 0{,}3\left(1-\left(1-\frac{1}{16}\right)^L\right)+0{,}7\left(1-\left(1-\frac{5}{16}\right)^L\right) \quad (4.26)$$

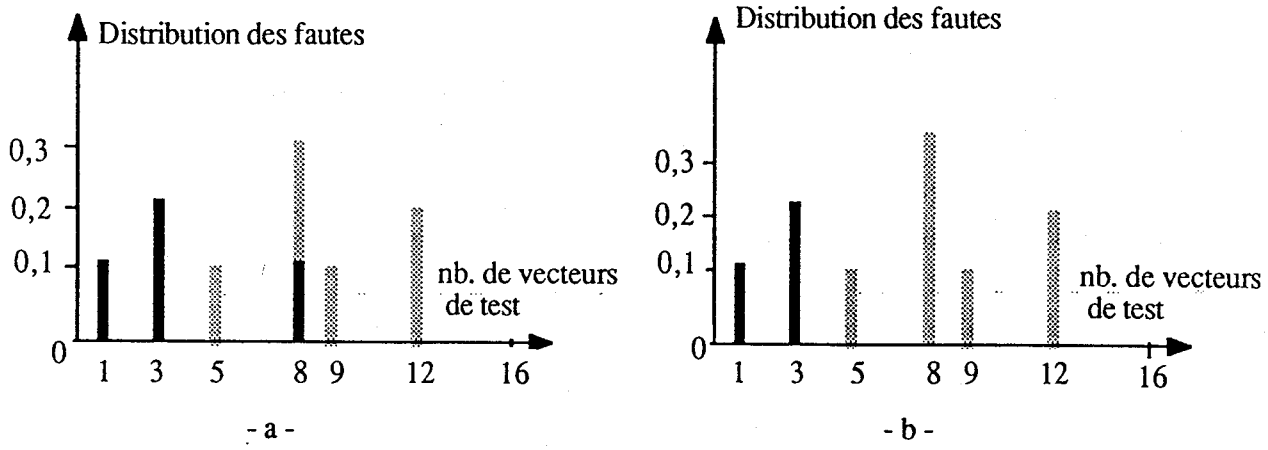


Figure 4.7 : Exemple fictif de 10 fautes
a - Distribution des blocs de ρ_1 b - Distribution des blocs de ρ_3

Pour **L = 90** on trouve $\mathbf{P_w(\rho_1) = 0{,}9988}$ et $\mathbf{P_w(\rho_3) = 0{,}9991}$. Soit $P_w(\rho_1) < P_w(\rho_3)$. Bien que ρ_1 et ρ_3 ne soient pas deux partitions comparables on peut dire que ρ_3 est une partition plus "efficace" que ρ_1 , c'est-à-dire que $P_w(\rho_3)$ est plus proche de P_a que $P_w(\rho_1)$.

Pour $P_w(\rho_3) = 0{,}999$ on trouve L = 89 (l'équation (4.21) conduit à 88,377 954 35). La partition ρ_2 définie dans l'exemple 4.5 est plus fine que ρ_3 ; néanmoins les équations (4.25) et (4.26) conduisent à la même longueur de test. Pour L = 90 on a :

$$\left(1-\frac{5}{16}\right)^L = 2{,}26\ 10^{-15}$$

Il suffit donc de montrer que f_4 est au moins aussi facile à tester que f_5.

□

Les différents critères que nous avons mentionnés plus haut permettent de réduire F_1 à un petit nombre de fautes. On peut alors envisager de calculer $P_a(F_1)$. Dans ce cas on peut calculer deux bornes de P_a qui sont très proches l'une de l'autre.

Propriété 4.1 : Soit $\rho = \{F_1, F_2\}$ une partition de F. On a :

$$Pr[F_2/F]\ P_m(F_2) + Pr[F_1/F]\ P_m(F_1) \le P_a \le Pr[F_2/F] + Pr[F_1/F]\ P_a(F_1)$$

Démonstration : Par définition on a :

$$P_w(\rho) = Pr[F_2/F]\, P_m(F_2) + Pr[F_1/F]\, P_m(F_1)$$

et d'après le corollaire 4.1 on a $P_w(\rho) \leq P_a$.

D'après le théorème 4.1 on a :

$$P_a = Pr[F_2/F]\, P_a(F_2) + Pr[F_1/F]\, P_a(F_1)$$

donc $P_a \leq Pr[F_2/F] + Pr[F_1/F]\, P_a(F_1)$

puisque $P_a(F_2) \leq 1$.

□

Exemple 4.10 : Pour l'exemple de 10 fautes déjà présenté et pour la partition ρ_3 définie dans l'exemple 4.9 ($\rho_3 = \{F_1, F_2\}$ avec $F_1 = \{f_1, f_2, f_3\}$ et $F_2 = \{f_4, f_5, f_6, f_7, f_8, f_9, f_{10}\}$) on a pour L = 89 :

$$\mathbf{0{,}999\,0 \leq P_a \leq 0{,}999\,7}$$

□

Pour le microprocesseur à test intégré étudié au chapitre 7 nous avons pu réduire suffisamment l'ensemble des fautes les plus difficiles à tester pour pouvoir calculer P_a à 10^{-7} près.

4 . 5 . Exemple d'application

Nous proposons d'illustrer les différentes propriétés que nous venons de mentionner sur un exemple simple. Soit le test aléatoire du circuit à 8 entrées présenté à la figure 4.8. Nous supposons que les 2^8 vecteurs d'entrée sont équiprobables et que les fautes qui peuvent affecter le circuit sont des collages simples.

Soit $F = \{f_1, ..., f_{34}\}$ l'ensemble des 34 collages sur les branches numérotées de 1 à 17. On notera q/0 et q/1 le collage à 0 et à 1respectivement de la branche numérotée q. On suppose de plus que les collages à 1 (resp. à 0) sont équiprobables et que le collage à 1 d'une branche est deux fois plus probable que le collage à 0 correspondant.

$$Pr[x/1 / F] = 2\, Pr[x/0 / F] \tag{4.27}$$

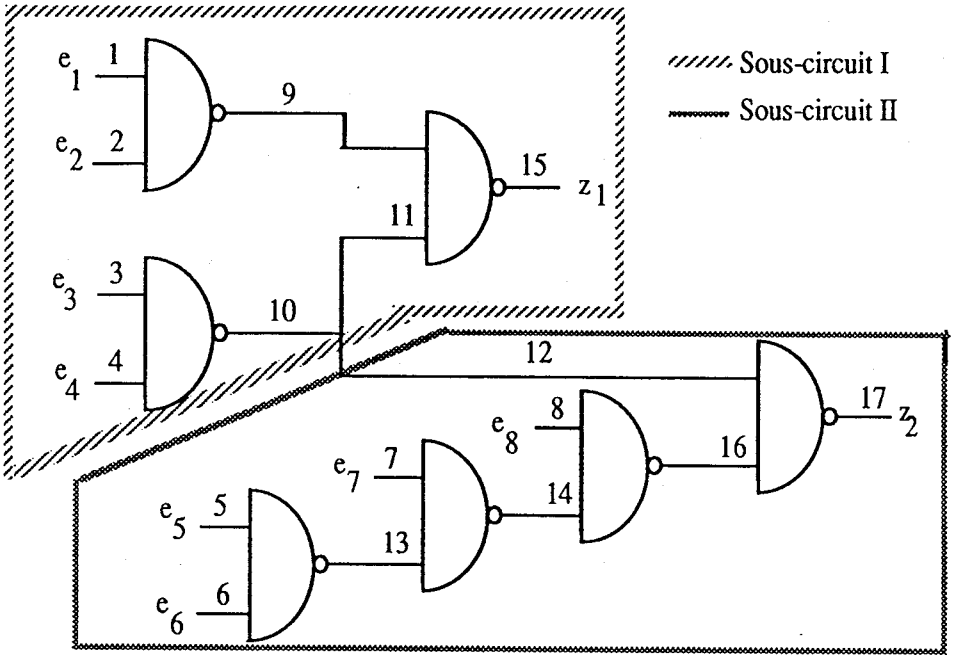
Le profil d'occurrence est donc le suivant :

$$\Omega = (Pr[1/0 / F], Pr[1/1 / F], Pr[2/0 / F], ..., Pr[17/1 / F])$$

$$\Omega = \left(\frac{1}{51}, \frac{2}{51}, \frac{1}{51}, \cdots, \frac{2}{51}\right) \tag{4.28}$$

Nous allons dans cette partie chercher à répondre à la question suivante : quelle est la longueur de la séquence de test qui permet de détecter au moins 999 circuits défectueux parmi 1 000 ? Il s'agit donc de trouver la plus petite valeur de L telle que $P_a \geq 0{,}999$. La méthode d'estimation que nous avons développée va permettre d'approcher L à moins de 2% près en ne

calculant la probabilité de test que de 2 fautes seulement.



- a -

Fautes	1/0	1/1	2/0	2/1	3/0	3/1	4/0	4/1	5/0	5/1	6/0	6/1	7/0	7/1	8/0	8/1
# vecteurs de test	48	48	48	48	59	59	59	59	12	12	12	12	36	36	60	60

Fautes	9/0	9/1	10/0	10/1	11/0	11/1	12/0	12/1	13/0	13/1	14/0	14/1	15/0	15/1	16/0	16/1	17/0	17/1
# vecteurs de test	144	48	177	59	144	48	132	44	36	12	60	36	112	144	132	60	124	132

- b -

Figure 4.8 : Exemple d'application
a - Circuit sous test. b - Nombre de vecteurs de test pour chaque faute.

Probabilité minimum pondérée de test

On peut distinguer dans le circuit testé deux sous-circuits définis par rapport aux sorties z_1 et z_2. Soit $\rho_1 = \{F_1, F_2\}$ la partition de F qui correspond à la décomposition réprésentée à la figure 4.8a. Soit F_1 l'ensemble des fautes qui affectent une branche en amont de z_1, soit F_2 l'ensemble des fautes qui affectent une branche en amont de z_2 et qui n'appartiennent pas à F_1. On

note 1/x l'ensemble des deux collages 1/0 et 1/1. On a alors :

$$F_1 = \{1/x, 2/x, 3/x, 4/x, 9/x, 10/x, 11/x, 15/x\}$$
$$F_2 = \{5/x, 6/x, 7/x, 8/x, 12/x, 13/x, 14/x, 16/x, 17/x\} \quad (4.29)$$

Les fautes les plus difficiles à tester dans F_1 sont les collages des entrées primaires e_1, e_2, e_3 et e_4. Pour tester la faute 1/0 il faut $e_1 = 1$, $e_2 = 1$ et la valeur 1 sur la ligne 11. Pour avoir 1 sur la ligne 11 on peut avoir $e_3\, e_4 = 00$ ou 01 ou 10. Les valeurs de $e_5\, e_6\, e_7$ et e_8 n'interviennent pas. On a donc trois valeurs possibles pour e_3 et e_4 et 16 valeurs possibles pour $e_5\, e_6 e_7 e_8$, soit un total de 48 vecteurs possibles. Autrement dit sur les 2^8 vecteurs d'entrée possibles (e_1, ..., e_8) il y en a 48 qui détectent la faute $e_1/0$. On trouve le même résultat pour $e_1/1$ et e_2/x. Les fautes e_3/x et e_4/x sont plus faciles à tester que e_1/x et e_2/x car ces fautes peuvent faire apparaître une erreur sur z_1 mais aussi sur z_2. L'ensemble des vecteurs de test pour e_1/x et e_2/x est donc inclus dans l'ensemble des vecteurs de test pour e_3/x et e_4/x. On a donc :

$$P_m(F_1) = \left(1 - \left(1 - \frac{48}{2^8}\right)^L\right) \quad (4.30)$$

Les fautes les plus difficiles à tester de F_2 sont les collages des entrées primaires e_5 et e_6. Par un raisonnement similaire à celui développé pour l'étude de $e_1/0$ on trouve que e_5/x et e_6/x sont testées par 12 vecteurs d'entrée. On a donc :

$$P_m(F_2) = \left(1 - \left(1 - \frac{12}{2^8}\right)^L\right) \quad (4.31)$$

Par ailleurs à partir du profil d'occurrence (équation (4.28)) et des relations (4.29) on peut calculer :

$$Pr[F_1/F] = \frac{8}{17} \quad \text{et} \quad Pr[F_2/F] = \frac{9}{17}$$

D'où :

$$P_w(\rho_1) = Pr[F_1/F]\, P_m(F_1) + Pr[F_2/F]\, P_m(F_2)$$
$$P_w(\rho_1) = \frac{8}{17}\left(1 - \left(1 - \frac{48}{2^8}\right)^L\right) + \frac{9}{17}\left(1 - \left(1 - \frac{12}{2^8}\right)^L\right) \quad (4.32)$$

Pour $P_w(\rho_1) = 0{,}999$ on trouve **L = 131**. L'équation (4.32) conduit à 130,636 711 14. Ce résultat nous permet de montrer que le sous-circuit I correspondant à F_1 est beaucoup plus facile à tester que le sous-circuit II correspondant à F_2. En effet pour L = 131 on a :

$$1 - P_m(F_1) = 1{,}53\ 10^{-12} \quad \text{et} \quad 1 - P_m(F_2) = 1{,}86\ 10^{-3}$$

On peut montrer de plus, que la longueur de test est déterminée par les fautes de F_2 qui

sont les plus difficiles à tester. En effet si on suppose que la séquence de test est un test complet pour le sous-circuit I, c'est-à-dire :

$$P_m(F_1) = 1$$

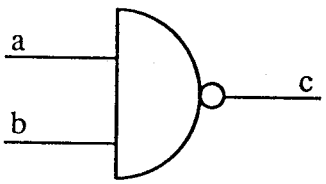
on a :

$$P_w'(\rho_1) = \frac{8}{17} + \frac{9}{17}\left(1 - \left(1 - \frac{12}{2^8}\right)^L\right) \qquad (4.33)$$

Pour $P_w'(\rho_1) = 0{,}999$ on trouve **L = 131**. L'équation (4.33) conduit à 130,636 711 00. Ce résultat diffère du résultat obtenu à partir de l'équation (4.32) à la septième décimale.

Les calculs précédents montrent que les **fautes les plus difficiles à tester déterminent le longueur de test.** Il faut donc les identifier le plus précisément possible. Les fautes de F_1 n'influent pas de manière significative sur la longueur de test. Il n'est donc pas nécessaire de les étudier en détail.

La plupart des fautes de F_2 sont testées par plus de 12 vecteurs d'entrée. Les propriétés connues sur les collages dans les circuits combinatoires permettent de l'affirmer. En particulier l'étude des **points de contrôle** du sous-circuit II permet de distinguer les fautes réellement difficiles à tester. Dans un circuit arborescent (il existe un chemin unique à partir d'une entrée primaire vers une des sorties observables du circuit) les points de contrôle sont les entrées primaires du circuit. Si le circuit contient des points de divergence (la branche 10 est un point de divergence par exemple) alors toutes les branches issues de ces points sont aussi des points de contrôle (les branches 11 et 12 sont des points de contrôle).



- a -

fautes / vecteurs de test	a/0	a/1	b/0	b/1	c/0	c/1
ab = 00					x	
ab = 01		x			x	
ab = 11	x		x			x
ab = 10				x	x	

- b -

Figure 4.9 : Test d'une porte Nand

Les points de contrôle du sous-circuit II sont les branches 5, 6, 7, 8 et 12. Si tous les collages qui peuvent affecter les points de contrôle sont testés alors tous les collages du circuit sont testés. On dit que *le test des points de contrôle couvre le test de toutes les fautes du circuit.* En

particulier le test du collage d'une ligne peut toujours être comparé avec le test du collage d'un point de contôle. Le tableau de la figure 4.9b donne les vecteurs de test de tous les collages simples qui peuvent affecter la porte Nand décrite à la figure 4.9a.

On voit sur ce tableau que si on teste "a" ou "b" collé à 0 alors on teste "c" collé à 1 et si on teste a/1 ou b/1 alors on teste c/0. Soit k(a/0) le nombre de vecteurs d'entrée qui testent la faute a/0. On a :

$$k(c/1) \geq k(a/0) \text{ et } k(b/0) \quad , \quad k(c/0) \geq k(a/1) \text{ et } k(b/1)$$

Si on utilise cette propriété pour chaque porte Nand du sous-circuit II on obtient les relations suivantes :

$$k(13/0) \geq k(5/1) \text{ et } k(6/1) \ , \ k(13/1) \geq k(5/0) \text{ et } k(6/0)$$
$$k(14/0) \geq k(7/1) \ , \ k(14/1) \geq k(7/0)$$
$$k(16/0) \geq k(8/1) \text{ et } k(14/1) \ , \ k(16/1) \geq k(8/0) \text{ et } k(14/0)$$
$$k(17/0) \geq k(12/1) \text{ et } k(16/1) \ , \ k(17/1) \geq k(12/0) \text{ et } k(16/0)$$

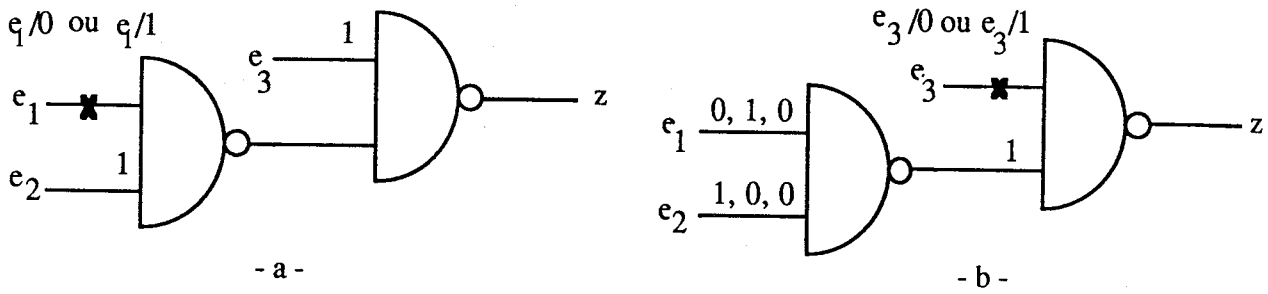


Figure 4.10 : Test des points de contrôle d'un réseau
a - b vecteurs de test des points de contrôle

L'exemple de deux portes Nand décrit à la figure 4.10 montre qu'un collage est d'autant plus difficile à tester qu'il affecte une branche proche des entrées primaires. En utilisant cette propriété on montre que (pour la figure 4.8):

$$k(8/0) \geq k(7/0) \text{ et } k(7/1) \ , \ k(8/1) \geq k(7/0) \text{ et } k(7/1)$$

Ces deux propriétés nous permettent de conclure que les fautes 8/x, 14/x, 16/x et 17/x sont au moins aussi faciles à tester que 7/x. Le raisonnement que nous avons détaillé pour la faute 1/0 appliqué aux fautes 7/0 et 7/1 permet de calculer k(7/0) = k(7/1) = 36

Soit $\rho_2 = \{F_1', F_2'\}$ la partition de F telle que :

$F_1' = \{1/x, 2/x, 3/x, 4/x, 7/x, 8/x, 9/x, 10/x, 11/x, 12/x, 14/x, 15/x\}$

$F_2' = \{5/x, 6/x, 13/x\}$

La probabilité minimum pondérée de test relative à cette partition s'écrit :

$$P_w(\rho_2) = Pr[F_1'/F]\left(1-\left(1-\frac{36}{2^8}\right)^L\right) + Pr[F_2'/F]\left(1-\left(1-\frac{12}{2^8}\right)^L\right) \qquad (4.34)$$

avec $Pr[F_1'/F] = \frac{14}{17}$ et $Pr[F_2'/F] = \frac{3}{17}$

Pour $P_w(\rho_2) = 0{,}999$ on trouve **L = 108**. L'équation (4.34) conduit à 107,754 7.

L'ensemble des fautes les plus difficiles à tester ne contient plus que 6 fautes parmi lesquelles 4 ont déja été étudiées pour trouver la probabilité minimum de test. Les deux fautes 13/0 et 13/1 sont les deux seules fautes éventuellement difficiles à tester dont on ne connait pas exactement la probabilité de test. A partir de l'étude d'une porte Nand présentée à la figure 4.9 on peut calculer très facilement :

$$k(13/0) = 3 \times 12 = 36 \quad \text{et} \quad k(13/1) = 12$$

La faute 13/0 n'est donc pas parmi les plus difficiles à tester. Soit $\rho_3 = \{F_1'', F_2''\}$ la partition de F telle que :

$$F_1'' = \{1/x, 2/x, 3/x, 4/x, 7/x, 8/x, 9/x, 10/x, 11/x, 12/x, 13/0, 14/x, 15/x\}$$

$$F_2'' = \{5/x, 6/x, 13/1\}$$

La probabilité minimum pondérée de test relative à la partition ρ_3 s'écrit :

$$P_w(\rho_3) = Pr[F_1''/F]\left(1-\left(1-\frac{36}{2^8}\right)^L\right) + Pr[F_2''/F]\left(1-\left(1-\frac{12}{2^8}\right)^L\right) \qquad (4.35)$$

avec $Pr[F_1''/F] = \frac{43}{51}$ et $Pr[F_2''/F] = \frac{8}{51}$

Pour $P_w(\rho_3) = 0{,}999$ on trouve **L = 106**. L'équation (4.35) conduit à 105,302 67.

Les fautes de F_2'' sont exactement connues. Dans ce cas particulier on a :

$$P_a(F_1'') = P_m(F_2'')$$

La propriété 4.1 s'écrit :

$$\frac{43}{51}\left(1-\left(1-\frac{36}{2^8}\right)^L\right) + \frac{8}{51}\left(1-\left(1-\frac{12}{2^8}\right)^L\right) \le P_a \le \frac{43}{51} + \frac{8}{51}\left(1-\left(1-\frac{12}{2^8}\right)^L\right) \qquad (4.36)$$

Soit pour L = 106 on a :

$$\mathbf{0{,}999\,032\,96 \le P_a \le 0{,}999\,033\,05}$$

Réciproquement les deux équations suivantes permettent de calculer deux bornes de la longueur de test à appliquer.

$$0{,}999 = \frac{43}{51}\left(1 - \left(1 - \frac{36}{2^8}\right)^L\right) + \frac{8}{51}\left(1 - \left(1 - \frac{12}{2^8}\right)^L\right)$$

$$0{,}999 = \frac{43}{51} + \frac{8}{51}\left(1 - \left(1 - \frac{12}{2^8}\right)^L\right)$$

Soit :

$$\mathbf{105{,}300 \leq L \leq 105{,}303}$$

Ce résultat très précis est obtenu à partir des informations suivantes :
1) chacune des fautes 5/0, 5/1, 6/0, 6/1, et 13/1 est testée par 12 vecteurs d'entrée.
2) chacune des 29 autres fautes est testée par au moins 36 vecteurs d'entrée.
3) tous les collages à 1 sont équiprobables, tous les collages à 0 sont équiprobables et les collages à 1 sont deux fois plus probables que les collages à 0.

4 . 6 . Remarques sur le domaine d'application

Cette méthode d'estimation de la confiance dans la séquence de test est particulièrement bien adaptée aux circuits qui ont **une structure modulaire.** La partition de l'ensemble de fautes suit alors la structure du circuit et la connaissance approfondie que l'on a le plus souvent des modules permet d'obtenir facilement les informations nécessaires au calcul de la probabilité minimum pondérée de test.

L'approche que nous proposons est d'autant plus efficace que le circuit testé est **hétérogène.** En effet pour un circuit qui serait composé de "n" sous-circuits identiques la décomposition du circuit en n sous-circuits ne permet pas d'améliorer l'estimation obtenue à partir de la probabilité minimum de test. Seule l'étude de chaque sous-circuit permet d'augmenter la précision du résultat. Si par contre le circuit est composé de blocs fonctionnels très différents la partition du circuit permettra de tirer profit du fait que certains sous-circuits sont plus faciles à tester que d'autres. La confiance dans la séquence de test sera connue de façon plus précise sans autre calcul que ceux nécessaires à la recherche du circuit le plus difficile à tester.

Le circuit MTI (Microprocesseur à Test Intégré) que nous étudions au chapitre 7 est un exemple réel qui permet d'apprécier l'efficacité de la méthode proposée. Il est composé de blocs fonctionnels très différents mais le sous-circuit qui contient la faute la plus difficile à tester est récursif. On verra sur cet exemple comment les critères de choix d'une partition proposés dans la

partie 4.4.2 s'appliquent à ces différentes structures.

La nouvelle approche d'estimation de la confiance dans la séquence de test qui est présentée dans ce chapitre s'appuie sur l'étude de partitions de l'ensemble de fautes. Elle conduit à des évaluations plus faciles à obtenir que la couverture des circuits défectueux tout en étant plus précise que la probabilité minimum de test. On montre de plus que les fautes les plus difficiles à tester déterminent la performance de la séquence de test.

Chapitre 5

Confiance dans un test compact

Dans ce chapitre les définitions formelles des mesures de la confiance dans un test sont étendues au cas où la réponse du circuit sous test compactée. Certaines propriétés sont démontrées. Dans le cas d'une analyse de signature des mesures de la confiance dans l'analyseur sont définies. Le cas du test compact statistique est également abordé.

5 . 1 . Introduction

Au cours d'une expérience de test et pour un circuit de taille réelle (microprocesseur, mémoire, ...) plusieurs milliers de vecteurs de test sont appliqués au circuit sous test (CST). Plusieurs milliers de bits sont alors disponibles en sortie du CST. Peu parmi eux permettent de détecter un circuit défectueux. En effet soit le test d'un circuit qui comprend 10 entrées et 4 sorties. Supposons que ce circuit soit affecté de la faute f_1 testée par 10 vecteurs d'entrée sur les $2^{10} = 1024$ vecteurs d'entrée possibles, et détectable sur une seule sortie. La séquence de test appliquée est une séquence aléatoire de 500 vecteurs. Les vecteurs d'entrée sont supposés équiprobables. L'espérance mathématique du nombre de bits faux, p_1, est égale à la proportion de vecteurs d'entrée qui testent f_1 multipliée par le nombre de vecteurs de test appliqué. Soit :

$$p_1 = \frac{10}{1024} \times 500 = 4{,}88$$

L'espérance mathématique de la proportion de bits faux, p_2, s'écrit alors :

$$p_2 = \frac{4{,}88}{500 \times 4} = 0{,}0024$$

Seulement 0,24 % des 4 x L bits de sortie permettent de détecter un circuit défectueux.

Le **test compact** consiste à construire une image compacte de la réponse du CST qui permette d'observer une erreur présente dans sette réponse. En d'autres termes il s'agit de concentrer, sur un nombre réduit de bits, l'information contenue dans la réponse et qui permet de détecter un circuit défectueux. Plusieurs méthodes d'observation de la réponse du CST ont été développées. Elles permettent de construire une image compacte de la réponse telle que sa valeur dépende de tous les bits de la réponse tout en garantissant une certaine simplicité de mise en oeuvre de l'observateur. La compactage* de la réponse revêt un intérêt tout particulier dans le cadre du test intégré. On cherche alors à réaliser des systèmes de test autonomes dans lesquels la comparaison

---

* Le terme utilisé en anglais est *compaction*. C'est un néologisme qui permet de ne pas utiliser le mot "compression" déjà utilisé en théorie de la communication et qui implique qu'il n'y a aucune perte d'information. Le compactage implique généralement une perte d'information.

avec un circuit sans faute se fait à partir d'une image enregistrée de ce circuit (obtenue par simulation ou par vote). Afin de ne pas occuper trop de place en mémoire, l'image enregistrée doit être aussi réduite que possible.

On peut distinguer deux types d'observation selon la nature de la séquence de test.
1) Si la séquence de test est **reproductible** (déterminise ou pseudo-aléatoire) on parle d'**analyse de signature.** L'image de la réponse du CST est appelée **signature** : un circuit conduit toujours à la même image si on répète l'expérience de test. Il existe deux classes de méthodes d'analyse de signature. Le test compact déterministe est presque toujours réalisé à l'aide d'une *méthode de comptage* (comptage de 1 ou de transitions). On utilise souvent un *registre à décalage à rebouclage linéaire* pour construire la signature d'un circuit testé à l'aide d'une séquence pseudo-aléatoire.
2) Si la séquence de test n'est **pas reproductible** (aléatoire non enregistrée ou que la signature n'a pas été prédéterminée) on parle de **test compact statistique.** A chaque expérience de test un circuit conduit à une image différente. En particulier on ne connait que les propriétés stastistiques de l'image d'un circuit sans faute : un circuit sans faute ne conduit pas toujours à la même image, il n'y a pas de référence. Soit par exemple le test aléatoire d'une porte ET à deux entrées. Le nombre moyen de "1" contenus dans la réponse, si les vecteurs d'entrée sont équiprobables, est égal à 0,25. Ce nombre est obtenu pour une longueur de test infinie. En général, pour une réalisation quelconque d'une séquence de test de longueur L, le nombre de "1" contenus dans la réponse n'est pas égal au quart du nombre de bits de la réponse.

Remarque 5.1 : Certaines méthodes de compactage s'accompagnent d'une augmentation du nombre de vecteurs de test à appliquer. La réduction du nombre de bits observés n'est de ce fait pas toujours très importante [Fujiwara 78]

□

L'efficacité d'un test compact dépend de trois facteurs principaux : la séquence de test, le circuit sous test et les fautes qui peuvent l'affecter, et le type d'observation. Ce chapitre est consacré à l'étude des mesures de la confiance dans un test compact appelée **confiance dans la méthode de test**. Nous verrons en particulier comment les 6 mesures présentées au chapitre 3 peuvent être généralisées à partir d'une image compacte de la réponse.

Dans le cas d'une *analyse de signature* les hypothèses de travail sont les mêmes pour le système global (séquence de test, CST et observateur) que pour l'observation directe de la réponse (séquence de test et CST seulement). Tous les circuits sans faute sont reconnus bons. Toutes les propriétés démontrées aux chapitres précédents restent vérifiées.

Dans le cas d'un *test compact statistique* certains circuits sans faute sont refusés. Les mesures de la confiance dans les circuits testés ne dépendent plus seulement du rendement de fabrication et de la capacité de la méthode de test à détecter un circuit défectueux mais elles sont aussi fonction de la proportion de circuits sans faute qui sont refusés. De ce fait les définitions et

propriétés énoncées au chapitre 3 ne peuvent pas toutes être étendues.

Après une partie consacrée aux définitions et notations utilisées dans ce chapitre nous étudierons dans la partie 5.2 le cas de l'analyse de signature. Dans un premier temps nous définirons les mesures de la confiance dans la méthode de test. Pour les dispositifs dans lesquels la séquence de test est construite par rapport à l'analyseur de signature utilisé (méthodes de comptage par exemple) l'étude de la confiance dans la méthode de test ne peut pas être plus développée. Pour les registres à décalage à rebouclage linéaire la génération de la séquence de test est indépendante de l'analyse de signature. La probabilité de détecter un circuit défectueux s'écrit en fonction de la probabilité de tester la faute présente dans le CST et de la probabilité de ne pas masquer l'erreur apparue dans la réponse. Cette décomposition nous permettra de démontrer certaines propriétés. Nous ferons ensuite une étude comparative de l'efficacité de la séquence de test et de l'efficacité de l'analyseur de signature. Le test compact statistique sera envisagé dans la partie 5.3. Il existe peu de propriétés dans ce cas. Il est néanmoins intéressant, d'un point de vue théorique, car les mesures de la confiance dans les circuits testés ont une écriture générale qui peut s'appliquer à une défaillance du dispositif de test.

5 . 2 . Hypothèses et notations

5 . 2 . 1 . Hypothèses

Le principe de test d'un circuit avec compactage de la réponse est décrit à la figure 5.1.

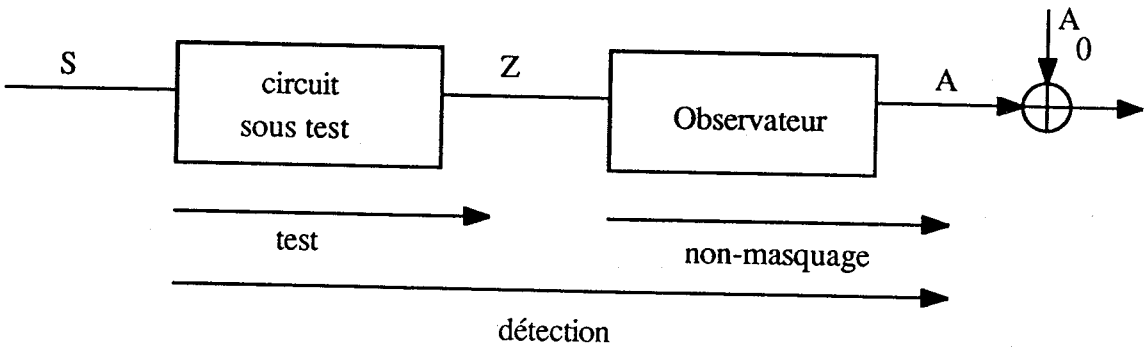


Figure 5.1 : Principe de test avec compactage de la réponse

La **séquence de test S** est appliquée au circuit sous test (CST). La **réponse Z** du CST est traitée par un système d'observation pour conduire à l'**image** notée **A**. L'image est une fonction compacte de la réponse. On notera A_i l'image d'un circuit qui contient la faute f_i, $i \neq 0$. Si

l'image d'un circuit sans faute est exactement connue on notera A_0 cette image (c'est le cas de l'analyse de signature). Si l'image d'un circuit sans faute n'est pas exactement connue on notera A_0^+ l'ensemble des images qui sont reconnues correctes par le dispositif de test (c'est le cas du test compact statistique).

5. 2 . 2 . Notions de base

Lorsque la séquence de test a fait apparaître une erreur en sortie d'un circuit défectueux et que ce circuit n'est pas détecté on dira qu'il y a eu **masquage** d'une réponse fausse. On parlera dans ce cas d'un **circuit défectueux masqué.**

On dira qu'un circuit est **passé** si aucune faute de F n'est détectée, c'est-à-dire si $A = A_0$ ou $A \in A_0^+$, sinon on dira qu'il est **refusé.** Ces définitions ne sont que la généralisation des définitions proposées au chapitre 3 pour lesquelles on a Z = A.

Par extension de la notion de résultat de test juste on dira que le **résultat de la détection** est **juste** si :

soit 1) le circuit est sans faute et passé

soit 2) le circuit est défectueux et refusé

La **probabilité de détecter** la faute f_i notée $\mathbf{P_D\ (f_i)}$, est la probabilité que le résultat de la détection soit juste lorsque la faute f_i est présente dans le CST.

$$P_D\ (f_i) = Pr\ [\text{le résultat de la détection est juste}/f_i] \qquad i \neq 0 \qquad (5.1)$$

5 . 3 . Analyse de signature

Le dispositif de test que nous nous proposons d'étudier dans cette partie a les propriétés suivantes :

1) la séquence de test est reproductible : déterministe ou pseudo-aléatoire,

2) l'image A_0 d'un circuit sans faute est entièrement connue.

Dans ces conditions un circuit sans faute conduit toujours à la même image qui est l'**image de référence A_0**, on parle d'**analyse de signature** et l'image du CST est appelée **signature.**

Propriété 5.1 : La probabilité de détecter la faute f_i peut s'écrire :

a) $P_D\ (f_0) = 1$

b) $P_D(f_i) = Pr[A_i \neq A_0]$ pour i = 1, ..., M

Démonstration : a) L'hypothèse 3.2 est vérifiée dans le cas de l'analyse de signature donc aucun circuit bon ne peut être refusé.

b) Si la faute f_i est présente dans le circuit sous test, le résultat de la détection est juste si une erreur apparaît dans la signature du circuit lorsque f_i est présente. On a donc pour $i \neq 0$:

$$P_D(f_i) = Pr[A \neq A_0/f_i] = Pr[A_i \neq A_0]$$

□

La figure 5.2 illustre les différents cas possibles suivant que le circuit est ou non défectueux.

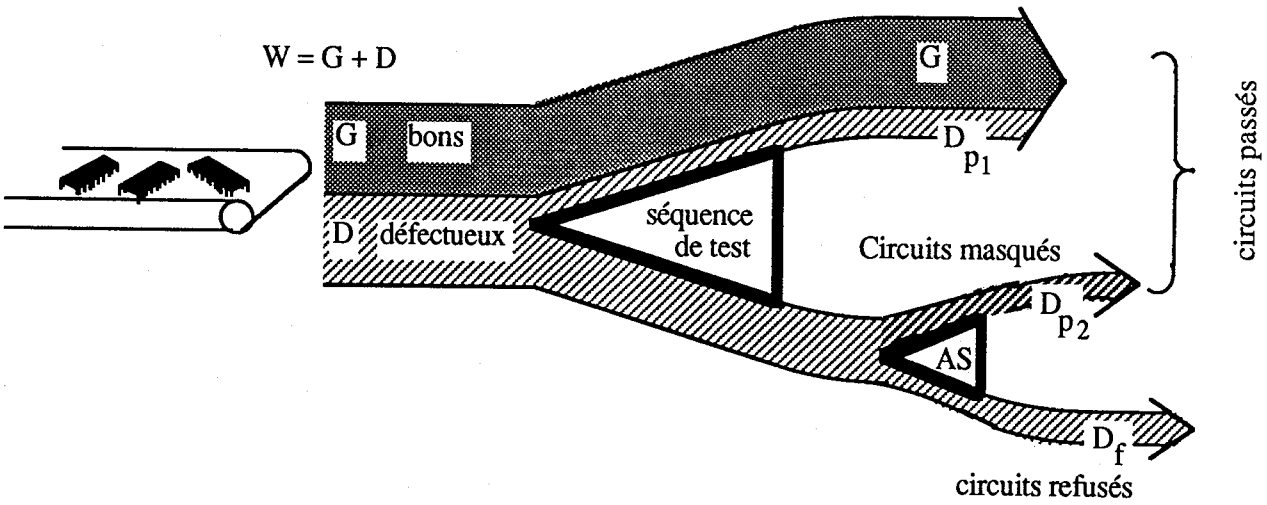


Figure 5.2 : Principe du test de circuits.

Les G circuits sans faute passent le test. Parmi les D circuits défectueux il y en a D_{p1} pour lesquels la séquence de test ne fait apparaître aucune erreur en sortie, il y en a D_{p2} pour lesquels la réponse fausse est masquée par l'analyseur de signature (ce sont les circuits masqués) et il y en a D_f qui sont détectés. On a donc $G + D_{p1} + D_{p2}$ circuits passés et D_f circuits refusés. Ce schéma de test est similaire à celui étudié dans les chapitres 3 et 4. On a maintenant $D_p = D_{p1} + D_{p2}$. Les six mesures que nous avons étudiées au chapitre 3 ainsi que la méthode approchée que nous avons présentée au chapitre 4 peuvent être étendues au cas de l'analyse de signature. Les propriétés que nous avons démontrées sont également vérifiées.

5 . 3 . 1 . Confiance dans les circuits testés

La proportion de circuits correctement testés et la proportion de circuits bons parmi les circuits passés sont les grandeurs qui intéressent le fabricant des circuits testés et l'utilisateur des circuits passés respectivement.

Définition 5.1 : La **confiance moyenne dans les circuits testés après signature** notée $*C_t$, est la probabilité que la détection soit juste lorsque la séquence de test S est appliquée.

$$*C_t = Pr \text{ [le résultat de la détection est juste]}$$

□

Dans le cas de l'analyse de signature un circuit sans faute ne peut être refusé. On a donc

$$Pr [A = A_0 / f_0] = P_D (f_0) = 1 \qquad (5.2)$$

En suivant la même démarche qu'au paragraphe 3.3 on peut calculer :

$$*C_t = Y + (1 - Y) Pr [A \neq A_0 / F] \qquad (5.3)$$

La confiance moyenne dans les circuits testés après signature s'écrit en fonction de la probabilité de refuser un circuit défectueux $Pr [A \neq A_0 / F]$. Toutefois cette probabilité ne caractérise plus seulement la capacité de la séquence de test à révéler un circuit défectueux, elle caractérise l'aptitude globale du dispositif de test à détecter un circuit défectueux ; c'est-à-dire la capacité conjointe de la séquence de test et de l'analyseur de signature à faire apparaître une signature fausse pour un circuit défectueux.

Définition 5.2 : La **couverture des circuits défectueux après signature** notée $*P_a$, est la probabilité de détecter la faute présente dans le CST sachant qu'il est défectueux.

$$*P_a = Pr [A \neq A_0 / F]$$

□

La couverture des circuits défectueux après signature peut s'écrire :

$$*P_a = Pr [A_1 \neq A_0] Pr [f_1/F] + ... + Pr [A_M \neq A_0] Pr [f_M/F] \qquad (5.4)$$

$$*P_a = P_D (f_1) Pr [f_1/F] + ... + P_D (f_M) Pr [f_M/F]$$

D'après l'équation 5.3 et la définition 5.2 on obtient la propriété suivante :

Propriété 5.2 : La confiance moyenne dans les circuits testés après signature est une fonction du rendement de fabrication et de la couverture des circuits défectueux après signature.

$$*C_t = Y + (1 - Y) *P_a$$

□

Définition 5.3 : La **confiance moyenne dans les circuits passés après signature** notée $*C_a$, est la probabilité qu'un circuit passé soit sans faute.

$$*C_a = Pr\,[f_0 / A = A_0]$$

□

Propriété 5.3 : La confiance moyenne dans les circuits passés après signature est une fonction du rendement de fabrication et de la couverture des circuits défectueux après signature.

$$*C_a = \frac{Y}{Y + (1 - Y)(1 - *P_a)}$$

Démonstration : On a :

$$Pr\,[f_0] = Pr\,[A = A_0]\,Pr\,[f_0 / A = A_0] + Pr\,[A \neq A_0]\,Pr\,[f_0 / A \neq A_0]$$

Tout circuit sans faute passe le test on a donc :

$$Pr\,[f_0 / A \neq A_0] = 0$$

et

$$Pr\,[f_0] = Pr\,[A = A_0]\,Pr\,[f_0 / A = A_0]$$

On peut donc écrire :

$$*C_a = Pr\,[f_0 / A = A_0] = \frac{Pr\,[f_0]}{Pr\,[A = A_0]}$$

On a de plus :

$$Pr\,[A = A_0] = Pr\,[f_0] + Pr\,[F]\,Pr\,[A = A_0 / F]$$

Ce qui peut s'écrire à partir de la définition 5.2 :

$$Pr\,[A = A_0] = Y + (1 - Y)(1 - *P_a)$$

□

Théorème 5.1 : Pour tout circuit, pour tout ensemble de fautes, pour toute séquence de test et pour tout analyseur de signature on a :

a) $*C_t \geq *P_a$, et $*C_t > *P_a$ si et seulement si $Y > 0$ et $*P_a < 1$

b) $*C_t \geq *C_a \geq Y$

c) $*C_t$ et $*C_a$ sont des fonctions croissantes de $*P_a$ pour tout Y tel que $0 < Y < 1$.

Démonstration : $*C_t$ et $*C_a$ s'écrivent en fonction de $*P_a$ et de Y de la même manière que C_t et C_a en fonction de P_a et Y. La démonstration du théorème 5.1 est donc similaire de celle du théorème 3.1.

□

Dans le cas d'une analyse de signature tous les circuits sans faute sont bien testés donc :

1) la proprtion de circuits bien testés $*C_t$ est au moins égale au rendement de fabrication Y. La proportion de circuits défectueux bien testés est la couverture des circuits défectueux après signature $*P_a$ donc $*C_t$ est au moins égale à $*P_a$.

2) si la méthode de test ne détectait aucun circuit défectueux alors la proportion des circuits passés bien testés $*C_a$ serait égale à Y. La capacité de la méthode de test à détecter un circuit défectueux permet de diminuer le nombre de circuits passés donc d'augmenter la proportion de circuits passés bien testés.

3) Aucun circuit refusé n'est mal testé donc la confiance moyenne dans les circuits testés (passés et refusés) est supérieure ou égale à la confiance moyenne dans les circuits passés.

5 . 3 . 2 . Confiance dans la méthode de test

Certains articles traitent de la capacité de la séquence de test à détecter un circuit défectueux, d'autres décrivent les performances d'un analyseur de signature. Nous proposons d'évaluer les performances du système pris dans son ensemble. Nous n'avons trouvé à ce jour aucun article qui traite de ce problème. Les mesures de confiance qui vont être définies dans cette partie sont donc nouvelles. Les différentes mesures de la confiance dans la séquence de test que nous avons présentées au chapitre 3 correspondent à différentes caractéristiques du dispositif de test. Par exemple on a $P_c = Pr [D_p = 0]$. On peut mesurer ces différentes caractéristiques lorsqu'un analyseur de signature est utilisé. On définit alors les mesures de la **confiance dans la méthode de test.**

Définition 5.4 : La probabilité de la couverture complète après signature notée $*P_c$, est la probabilité que chaque faute de F conduise à une signature fausse.

$$*P_c = Pr [(A_1 \neq A_0) \text{ et } ... \text{ et } (A_M \neq A_0)]$$

□

La probabilité de la couverture complète après signature est le critère d'efficacité implicitement retenu par les auteurs qui développent les méthodes d'analyse de signature dépendantes de la séquence de test.

Hayes dans [Hayes 76] traite de l'analyse de signature par **comptage de transitions.** La signature du CST est le nombre de passages de la valeur logique 0 à la valeur logique 1, ou inversement, contenu dans sa réponse. Plusieurs réponses différentes peuvent conduire à la même signature, par exemple la signature correcte et son complémentaire bit à bit. Pour les circuits non redondants à deux niveaux qui peuvent être affectés par des collages Hayes décrit les séquences de test qui conduisent à une couverture complète après signature.

La méthode de test étudiée par Savir dans [Savir 80] comprend un test exhaustif du circuit et une analyse de signature par comptage de 1 (**syndrome**). En ajoutant dans le circuit des entrées qui ne sont mises à 1 que lors du test l'auteur montre que tous les collages simples d'un

circuit non redondant sont détectés par le nombre de 1 contenu dans la réponse du CST obtenue lors d'un test exhaustif.

Le nombre de 1 est un coefficient particulier du spectre de Rademacher-Walsh d'une fonction logique. Une fonction à n variables est entièrement déterminée par ses 2^n *coefficients de spectre*. Miller et Mizuo dans [Miller 84] d'une part et Susskind dans [Susskind 83] d'autre part utilisent cette propriété pour détecter un circuit défectueux. La signature du circuit sous test est tout ou partie de son spectre de Rademacher-Walsh. Le calcul de plusieurs coefficients de spectre permet de détecter tous les collages simples.

Il apparaît clairement que bien qu'aucun des auteurs cités ne cherche à mesurer l'efficacité de la méthode qu'il propose, tous construisent une méthode qui assure la détection de chaque collage simple, soit $*P_c = 1$ si l'ensemble de fautes prescrit est l'ensemble des collages simples.

Définition 5.5 : La **couverture de fautes espérée après signature** notée $*P_E$, est la moyenne arithmétique du nombre de fautes qui conduisent à une signature fausse.

$$*P_E = \frac{Pr\,[A_1 \neq A_0] + \ldots + Pr\,[A_M \neq A_0]}{M}$$

□

Cette notion n'a jamais été utilisée à notre connaissance. Par contre de nombreux auteurs prennent comme hypothèse de travail l'équiprobabilité de toutes les réponses incorrectes ([Hayes 76], [Frohwerk 77], [Agrawal 83], [Hassan 84]). Il n'existe aucun lien entre cette hypothèse et l'ensemble de fautes prescrit. Néanmoins cette hypothèse a permis dans certains cas d'améliorer la méthode de test. En effet dans [Hayes 76] l'auteur calcule le nombre de réponses fausses qui contiennent le même nombre de transistions que la réponse correcte parmi toutes les réponses fausses qui existent (toutes ne sont pas possibles en réalité). Ce nombre est maximum lorsque la signature de référence est égale à L/2. L'auteur utilise cette propriété pour construire des séquences de test qui conduisent à un nombre minimum de transitions dans la réponse correcte.

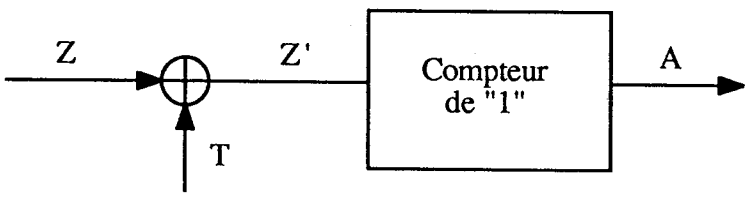


Figure 5.3 : Analyse de signature par modification de données

Agrawal dans [Agrawal 83] traite de l'analyse de signature par **modification des données de la réponse.** La méthode consiste à modifier la réponse du CST en calculant la

disjonction entre la réponse Z et une séquence de modification T (figure 5.3). La signature du CST est le nombre de 1 contenu dans la réponse modifiée Z'. Si toutes les réponses fausses sont équiprobables la probabilité de ne pas détecter un circuit défectueux (le nombre de 1 dans Z' est le même que dans Z_0') est maximum lorsque la signature correcte est proche de L/2. Agrawal utilise cette propriété pour construire la séquence de modification T telle que la signature d'un circuit sans faute soit différente de L/2.

Définition 5.6 : La **probabilité minimum de test après signature** (ou **probabilité minimum de détection**) notée $*P_m$, est la probabilité minimum de détecter un circuit défectueux sachant qu'il est défectueux.

$$*P_m = \min (Pr [A_1 \neq A_0], ..., Pr [A_M \neq A_0])$$

□

A notre connaissance cette mesure n'a jamais été utilisée. Trouver la faute la plus difficile à détecter n'est pas trivial. En effet en général la probabilité de ne pas masquer une faute f_i dépend de manière non monotone de la probabilité de tester la faute f_i. La faute la plus difficile à tester n'est donc pas forcément la faute la plus difficile à détecter, (par exemple plusieurs bits erronés peuvent s'effacer mutuellement). Nous verrons au chapitre 7 sur un exemple l'influence de la longueur de test et de la probabilité de test d'une faute f_i sur la probabilité que cette faute ne soit pas masquée.

Les définitions précédentes permettent de démontrer qu'il existe certaines relations d'ordre entre les différentes mesures de la confiance dans la méthode de test.

Théorème 5.2 : Pour tout circuit, pour tout ensemble de fautes, pour toute séquence de test et pour tout analyseur de signature on a :

a) $*P_a (\Omega_e) = *P_E$

b) $*P_E$ et $*P_a \geq *P_m \geq *P_c$

Démonstration : La démonstration de ce théorème est similaire à celle du théorème 3.2 car les différentes mesures de la confiance dans la méthode de test s'écrivent en fonction de la signature A du CST de la même manière que les mesures de la confiance dans la séquence de test s'écrivent en fonction de la réponse Z.

□

Le théorème 5.2 permet de comparer les différentes mesures de la confiance dans la méthode de test. Le tableau de la figure 5.4 indique l'information nécessaire au calcul de chacune de

ces mesures.

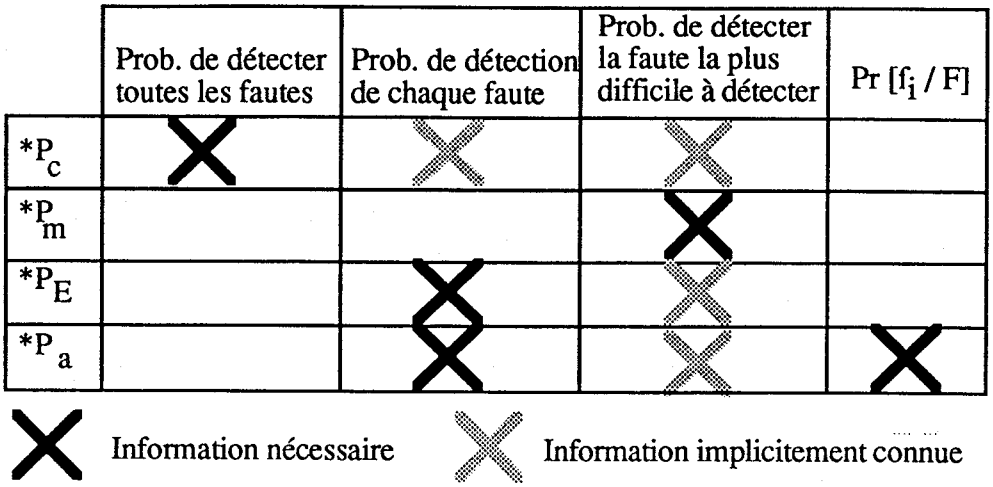


Figure 5. 4 : Information nécessaire pour obtenir les mesures de la confiance dans la méthode de test

Rappelons que la probabilité de détecter le faute f_i caractérise la capacité conjointe 1) de la séquence de test à détecter un circuit affecté de la faute f_i, et 2) de l'analyseur de signature à ne pas masquer l'erreur apparue en sortie du CST lorsque la faute f_i est présente et testée. La difficulté de calcul des différentes probabilités de détection dépend quant à elle de l'analyseur de signature utilisé. Nous détaillerons cet aspect dans les parties suivantes consacrées à l'étude des propriétés relatives à chaque analyseur de signature. Néanmoins on peut affirmer que pour un analyseur donné on a les relations suivantes : (I ($*P_x$) représente l'information nécessaire pour obtenir la mesure $*P_x$)

$$I(*P_c) \text{ et } I(*P_a) \supset I(*P_E) \supset I(*P_m)$$

$I(*P_a)$ et $I(*P_c)$ ne sont pas comparables.

La probabilité minimum de test après signature est donc la mesure la plus facile à obtenir alors que la mesure la plus significative est la couverture des circuits défectueux après signature. La méthode approchée d'estimation de la confiance dans la séquence de test que nous avons présentée au chapitre 4 peut être étendue au cas de l'analyse de signature.

5 . 3 . 3 . Méthode approchée d'estimation de la confiance dans la méthode de test

Les mesures de la confiance dans la méthode de test peuvent être définies sur tout sous-ensemble de F. On peut en particulier définir la probabilité minimum de test après signature sur tout sous-ensemble F_j de F.

Définition 5.7 : Soit $F_j = \{f_1^j, ..., f_{nj}^j\}$ un sous-ensemble de F. La **probabilité minimum de test après signature sur F_j** notée $*P_m (F_j)$, est la probabilité minimum de détecter un circuit défectueux sachant qu'une faute de F_j est présente.

$$*P_m (F_j) = \min (Pr [A_1^j \neq A_0], ... Pr [A_{nj}^j \neq A_0])$$

□

Définition 5.8 : Soit ρ une partition de F, $\rho = \{F_1, ..., F_r\}$. La **probabilité minimum pondérée de test après signature** (ou **probabilité minimum pondérée de détection**) relative à la partition ρ notée $*P_w (\rho)$, est la moyenne des probabilités minimum de détection sur ρ pondérée par la probabilité d'occurrence de chacun des blocs de ρ.

$$*P_w (\rho) = Pr [F_1/F] *P_m (F_1) + ... + Pr [F_r/F] *P_m (F_r)$$

□

Pour obtenir $*P_w (\rho)$ il faut calculer les probabilités minimum de détection sur les blocs de ρ et les probabilités d'occurrence de ces blocs. En termes de fautes il faut connaître la probabilité de détecter la faute la plus difficile à détecter de chaque bloc et la probabilité que la faute qui affecte le circuit appartienne à chacun de ces blocs.

A partir du tableau de la figure 5.5 on voit que

$$I (*P_a) \supset I (*P_w (\rho)) \supset I (*P_m)$$

	Prob. de détection de chaque faute	Prob. de détecter la faute la plus difficile à détecter de chaque bloc F_i	Prob. de détecter la faute la plus difficile à détecter	Pr [f_i / F]	Pr [F_i / F]
$*P_a$	X	X	X	X	X
$*P_m$			X		
$*P_w (\rho)$		X	X		X

X Information nécessaire X Information implicitement connue

Figure 5.5 : Information nécessaire au calcul de la probabilité minimum pondérée de détection

Théorème 5.3 : Pour tout circuit, pour tout ensemble de fautes, pour toute séquence de test, pour tout analyseur de signature et pour toutes partitions ρ_1 et ρ_2 on a :

a) si $\rho_1 \leq \rho_2$ alors $*P_w (\rho_1) \geq *P_w (\rho_2)$

b) $*P_w (0) = *P_a$

c) $*P_w (I) = *P_m$

Démonstration : La démonstration de ce théorème est similaire à la démonstration du théorème 4.2 dans laquelle la probabilité de test Pr $[Z_i \neq Z_0]$ est remplacée par la probabilité de détection Pr $[A_i \neq A_0]$.

□

Corollaire 5.1 : Pour tout circuit, pour tout ensemble de fautes, pour toute séquence de test, pour tout analyseur de signature et pour toute partition ρ on a :

$$*P_m \leq *P_w(\rho) \leq *P_a$$

Démonstration : Ce corollaire se déduit immédiatement du théorème 5.3 car $0 < \rho < I$ pour toute partition ρ.

□

Un ensemble de fautes les plus difficiles à détecter intervient dans le calcul de $*P_w(\rho)$ non plus seulement la faute la plus difficile à détecter comme dans $*P_m$. La probabilité minimum pondérée de détection approche d'autant mieux $*P_a$ que la partition ρ est plus efficace. En pratique une étude précise des seules fautes les plus difficiles à détecter suffit pour estimer $*P_a$.

5 . 3 . 4 . Comparaison avec l'information contenue dans la réponse

La compactage de la réponse ne se fait pas sans perte d'information. Certains circuits défectueux correctement testés ne sont pas détectés du fait de l'analyse de signature : ce sont les D_{p2} circuits masqués (figure 5.2). L'analyse de signature est un processus imparfait qui diminue la qualité du résultat du test.

Théorème 5.4 : Pour tout circuit, pour tout ensemble de fautes, pour toute séquence de test, pour tout analyseur de signature et pour toute partition ρ la confiance de test après signature est inférieure ou égale à la confiance de test lorsque la réponse du CST est directement observée.

a) $*P_c \leq P_c$ b) $*P_E \leq P_E$ c) $*P_m \leq P_m$ d) $*P_a \leq P_a$

e) $*C_t \leq C_t$ f) $*C_a \leq C_a$

g) $*P_w(\rho) \leq P_w(\rho)$

Démonstration : Toute signature incorrecte provient d'une réponse incorrecte :

$$A \neq A_0 \Rightarrow Z \neq Z_0$$

donc

$$\Pr[A \neq A_0] \leq \Pr[Z \neq Z_0] \qquad (5.5)$$

ce qui peut aussi s'écrire :

$$\forall\ i = 1, ..., M \quad Pr\,[A_i \neq A_0] \leq Pr\,[Z_i \neq Z_0] \tag{5.6}$$

a) $*P_c \leq P_c$ **:** D'après la définition 5.4 on a :

$$*P_c = Pr\,[(A_1 \neq A_0) \text{ et } ... \text{ et } (A_M \neq A_0)]$$
$$\leq Pr\,[(Z_1 \neq Z_0) \text{ et } ... \text{ et } (Z_M \neq Z_0)] = P_c$$

car $(A_1 \neq A_0)$ et ... et $(A_M \neq A_0) \Rightarrow (Z_1 \neq Z_0)$ et ... et $(Z_M \neq Z_0)$.

b) $*P_E \leq P_E$ **:** D'après la définition 5.5 on a :

$$*P_E = \frac{Pr\,[A_1 \neq A_0] + ... + Pr\,[A_M \neq A_0]}{M}$$
$$\leq \frac{Pr\,[Z_1 \neq Z_0] + ... + Pr\,[Z_M \neq Z_0]}{M} = P_E$$

d'après la relation (5.6).

c) $*P_m \leq P_m$ **:** Supposons que f_1 soit la faute la plus difficile à détecter et que f_2 soit la faute la plus difficile à tester. On a alors :

$$*P_m = Pr\,[A_1 \neq A_0] \quad \text{et} \quad P_m = Pr\,[Z_2 \neq Z_0]$$

De plus

$$Pr\,[A_2 \neq A_0] \geq Pr\,[A_1 \neq A_0]$$

D'après la relation (5.6) on obtient :

$$Pr\,[A_1 \neq A_0] \leq Pr\,[A_2 \neq A_0] \leq Pr\,[Z_2 \neq Z_0]$$

Soit

$$*P_m \leq P_m$$

d) $*P_a \leq P_a$ **:** D'après l'équation (5.4) on a :

$$*P_a = Pr\,[A_1 \neq A_0]\ Pr\,[f_1/F] + ... + Pr\,[A_M \neq A_0]\ Pr\,[f_M/F]$$

En utilisant l'équation (5.5) on peut écrire :

$$*P_a \leq Pr\,[Z_1 \neq Z_0]\ Pr\,[f_1/F] + ... + Pr\,[Z_M \neq Z_0]\ Pr\,[f_M/F] = P_a$$

e) f) sont évidents à partir de d) et des propriétés 5.2 et 5.3

g) est évident à partir de c) et de la définition 5.8.

□

Cette propriété montre que l'imperfection du test est en partie due à l'analyse de signature. Les différences $P_x - *P_x$ et $C_x - *C_x$ permettent d'estimer la perte de confiance due à l'analyse de signature. Néanmoins lorsque la génération des vecteurs de test dépend de l'analyseur de signature il me paraît tout à fait arbitraire de décomposer le dispositif de test en deux systèmes pour en mesurer la confiance : la séquence de test et l'analyseur de signature.

Sur le plan mathématique on peut écrire :

$$\forall\ i = 1, ..., M,\quad Pr\,[A_i \neq A_0] = Pr\,[\,A_i \neq A_0 / Z_i \neq Z_0]\ Pr\ [Z_i \neq Z_0] \qquad (5.7)$$

car $A_i \neq A_0 \Rightarrow Z_i \neq Z_0$, c'est-à-dire que $Pr\,[\,A_i \neq A_0 / Z_i = Z_0] = 0$

Dans cette équation on a $Pr\,[A_i \neq A_0] = P_D\,(f_i)$ la probabilité de détecter la faute f_i sachant qu'elle affecte le CST et $Pr\ [Z_i \neq Z_0] = P_T\,(f_i)$ la probabilité que la séquence de test fasse apparaître une erreur en sortie du CST sachant que f_i est présente. Le terme $Pr\,[\,A_i \neq A_0 / Z_i \neq Z_0]$ représente la capacité de l'analyseur de signature à ne pas masquer une réponse fausse. Cette probabilité n'a de sens que si l'analyse de signature est indépendante de la génération des vecteurs de test.

Exemple : Supposons tester une porte ET à deux entrées (figure 5.6a) qui peut être affectée des fautes de l'ensemble F suivant :

$$F = \{f_1, f_2, f_3, f_4, f_5, f_6\} = \{a/1, a/0, b/1, b/0, c/1, c/0\}$$

q/i représente le collage à i = 1 ou 0 de la ligne q.

La signature du CST est le nombre de transitions contenues dans la réponse. La mise en oeuvre d'une méthode de comptage s'accompagne généralement d'une génération déterministe des vecteurs de test. Soit l'ensemble de vecteurs d'entrée suivant :

$$\{X_1, X_2, X_3\} = \{10, 01, 11\}$$

avec X_i = ab. Cet ensemble assure une couverture complète de F.

Cas 1 : Soit la séquence de test $S_1 = X_1X_2X_3$. La réponse d'un circuit sans faute est $Z_0 = 001$ et $A_0 = 1$ (figure 5.6a). Supposons que l'entrée "a" de la porte ET soit collée à 1, la faute f_1 est présente dans le CST. On a alors $Z_1 = 011$ et $A_1 = 1$. Le circuit sans faute et le circuit défectueux ont la même signature bien qu'une erreur apparaisse dans la réponse du CST. Il y a donc **masquage** d'un circuit défectueux.

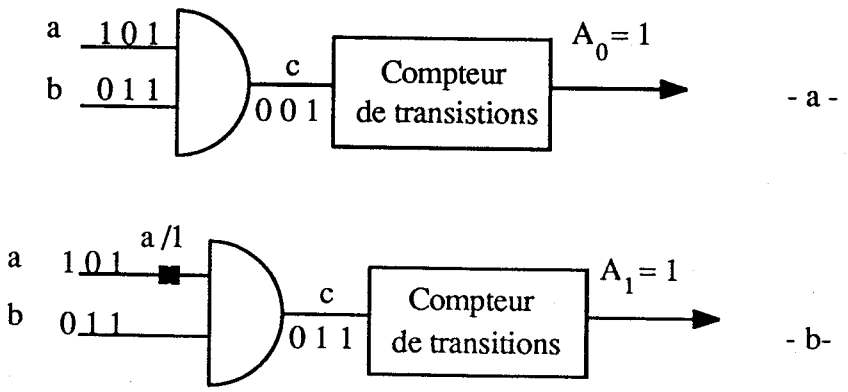


Figure 5.6 : Test par comptage de transitions
a - Porte sans faute b - Porte défectueuse

Cas 2 : Soit la séquence de test $S_2 = X_2X_3X_1$. La réponse d'un circuit sans faute est $Z_0 = 010$ et sa signature $A_0 = 2$. La réponse d'un circuit affecté de la faute f_1 est $Z_1 = 110$ et sa signature $A_1 = 1$ (figure 5.7).

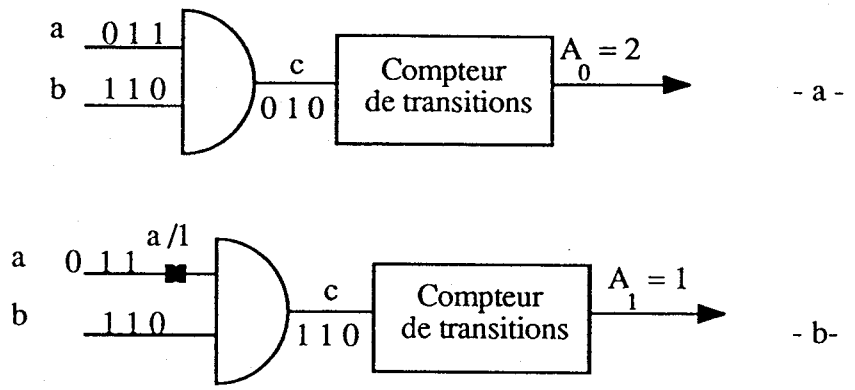


Figure 5.7 : Test par comptage de transitions
a - Porte sans faute b - Porte défectueuse

La séquence S_2 permet de détecter la faute f_1.

□

Dans ces deux cas la séquence de test fait apparaître une erreur en sortie du circuit défectueux mais seule la séquence S_2 permet de détecter la faute f_1 du fait de l'analyse de signature. Les deux séquences S_1 et S_2 conduisent à $Z_1 \neq Z_0$ avec un seul bit faux dans Z_1 . Pourtant cet événement ne permet pas toujours de détecter la faute f_1. On voit donc sur cet exemple que $Pr\,[A_i \neq A_0/Z_i \neq Z_0]$ ne peut pas être calculé.

Lorsque l'analyse de signature est indépendante de la génération des vecteurs de test la capacité de l'analyseur de signature à détecter un circuit défectueux dépend du nombre de bits faux disponibles en sortie du CST.

5 . 3 . 5 . Génération des vecteurs de test indépendante de l'analyse de signature : les registres à décalage à rebouclage linéaire

L'étude que nous avons développée jusque là est générale. Les résultats obtenus peuvent être appliqués quel que soit l'analyseur de signature utilisé. Pour certaines méthodes d'analyse de signature la performance de l'analyseur dépend entièrement de la séquence appliquée (méthodes de comptage). Pour d'autres méthodes d'analyse de signature la performance de l'analyseur dépend des propriétés statistiques de la réponse. On peut, dans ce cas, étudier l'efficacité propre de l'analyseur de signature. Les définitions et propriétés inhérentes à ce cas sont développées dans cette partie. L'analyse de signature à l'aide de registres à décalage à rebouclage linéaire, qui est la méthode la plus utilisée, illustrera notre propos.

Deux types d'opérateurs composent un registre à décalage à rebouclage linéaire : les bascules D et les portes OU exclusif. Les bascules connectées en série constituent un registre à décalage. La disjonction entre les sorties de certaines bascules ramenées en entrée du registre conduit à un **registre à décalage à rebouclage linéaire** appelé **LFSR** de l'anglais Linear Feedback Shift Register (figure 5.8).

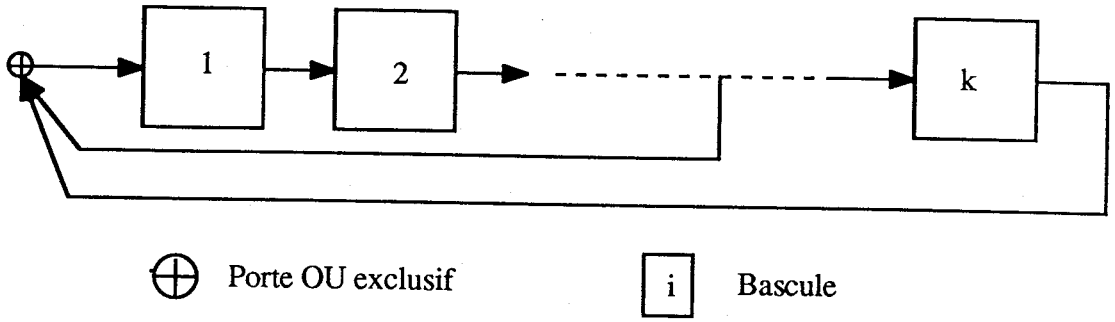


Figure 5.8 : Un registre à décalage à rebouclage linéaire (LFSR)

Lorsqu'un registre à décalage à rebouclage linéaire est utilisé comme analyseur de signature (figure 5.9) une expérience de test se déroule de la façon suivante. Le contenu du registre est initialisé avant que la séquence de test ne soit appliquée. Les vecteurs de test sont ensuite appliqués au CST de façon synchrone avec le décalage des données dans le registre de signature. Cela signifie que le premier vecteur de test est appliqué au CST. Après un certain temps le résultat est disponible en sortie du CST et à l'entrée du registre. Les données sont décalées d'un cran vers la droite dans le registre. Le second vecteur de test peut alors être appliqué au circuit. La signature du CST est le contenu du registre lorsque toute la séquence de test a été appliquée.

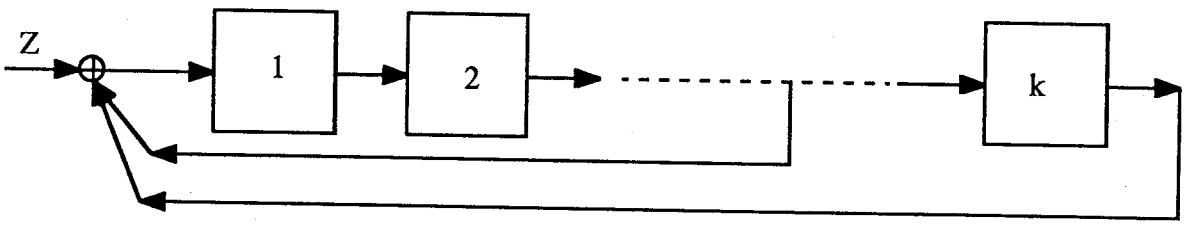


Figure 5.9 : LFSR utilisé comme analyseur de signature

Dans le cas général la capacité d'un LFSR à ne pas masquer de réponse fausse dépend du nombre de bascules qui le composent, des rebouclages effectués, de la longueur de la séquence de test et de la proportion de bits faux dans la réponse du CST. Les propriétés statistiques de la réponse du CST permettent de mesurer la performance de l'analyseur de signature [David 80], [David 86] et [Williams 86].

Les problèmes du test et de l'observation du circuit peuvent être dissociés. En termes de

confiance le dispositif de test (séquence et analyseur) peut être étudié comme un système composé de deux éléments : la *séquence de test* appliquée au CST et l'*analyseur de signature*.

Le schéma de la figure 5.10 met en évidence, du point de vue du fonctionnement, le fait que la séquence de test et l'analyseur de signature ne sont pas de même nature. Néanmoins du point de vue de la confiance dans le test la séquence de test et l'analyseur de signature sont deux composants qui servent à distinguer les circuits bons des circuits défectueux.

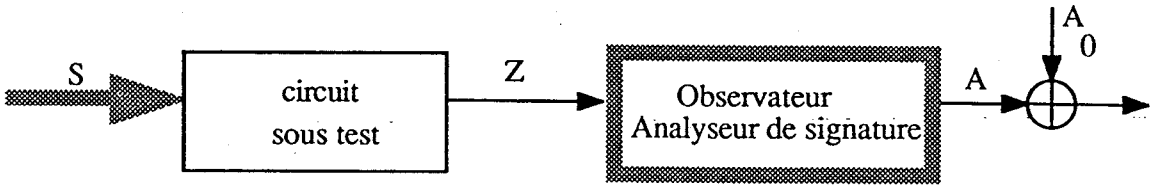


Figure 5.10 : Le dispositif de test est composé de 2 éléments :
la séquence de test et l'analyseur de signature.

Afin de mesurer la confiance dans l'analyseur de signature nous proposons de modéliser le système d'observation de la réponse de manière analogue au test du CST par la séquence de test. Soit S l'application qui fait correspondre une réponse Z_i à un circuit affecté de la faute f_i lorsque la séquence S est appliquée. On peut, de la même façon, appeler C l'application qui fait correspondre une signature A_i à une réponse Z_i lorsque l'analyse de signature est réalisée par un registre à décalage à rebouclage linéaire. On a donc :

$$Z_i = S\ (f_i)$$
$$A_i = C\ (Z_i)$$

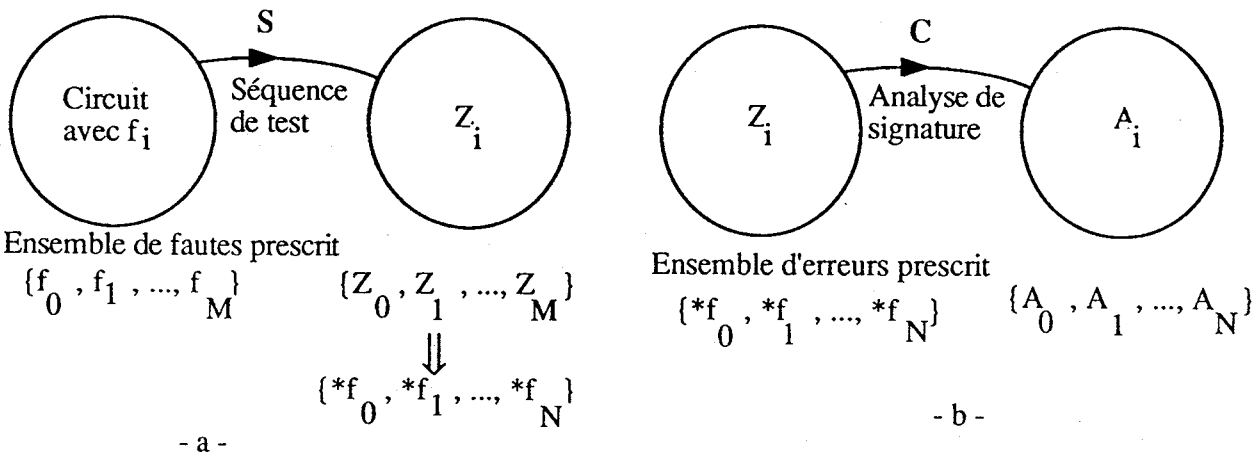


Figure 5.11 : Modélisation
a - Séquence de test b - Analyse de signature

Une analyse de signature est appliquée à l'ensemble des réponses obtenues afin de distinguer les réponses correctes des réponses fausses. La signature A correspondant à la réponse Z est comparée à la signature A_0 correspondant à la réponse correcte Z_0 (figure 5.11).

La performance de l'analyseur de signature est relative à un ensemble de réponses fausses possibles : on parlera d'**ensemble d'erreurs prescrit** par analogie avec l'*ensemble de fautes prescrit*. La probabilité $\mathbf{Pr\ [A \neq A_0 / Z \neq Z_0]}$ caractérise la **capacité de l'analyseur de signature** à détecter une réponse fausse. Cette probabilité a maintenant un sens. On notera $\mathbf{P_A\ (f_i) = Pr\ [A_i \neq A_0 / Z_i \neq Z_0]}$ la **probabilité de non-masquage** de la faute f_i. A partir de ce modèle on peut définir les mesures de la confiance dans l'analyseur de signature.

a - Confiance dans l'analyseur de signature :

Définition 5.9 : La **probabilité de la couverture complète des réponses fausses** notée P_{Ac}, est la probabilité que la signature soit fausse pour toute réponse fausse possible.

$$P_{Ac} = Pr\ [(A_1 \neq A_0 / Z_1 \neq Z_0) \text{ et } ... \text{ et } (A_M \neq A_0 / Z_M \neq Z_0)]$$

□

Pour réaliser la couverture complète des réponses fausses il faut construire un analyseur de signature qui détecte toutes les réponses fausses, ce qui n'est pas possible dans le cas général.

Soit $F = \{f_1, ..., f_M\}$ l'ensemble de fautes prescrit. Les fautes f_i et f_j sont **distinguables** par la séquence S si $Z_i \neq Z_j$ lorsque la séquence S est appliquée. Soit $*F = \{*f_1, ..., *f_N\}$, $N < M$, l'ensemble des classes de fautes de F distinguables par S. Une classe $*f_i$ représente soit une faute de F, soit un ensemble de fautes de F non distinguables par S. Les propriétés statistiques de l'ensemble des erreurs possibles se déduisent des propriétés statistiques de l'ensemble de fautes *F distinguables par S. En particulier l'équiprobabilité des réponses fausses possibles correspond à l'équiprobabilité des classes de fautes distinguables par S.

Définition 5.10 : La **couverture d'erreurs espérée** notée P_{AE}, est l'espérance mathématique du nombre de réponses fausses détectées.

$$P_{AE} = \frac{Pr\ [A_1 \neq A_0 / Z_1 \neq Z_0] + ... + Pr\ [A_M \neq A_0 / Z_M \neq Z_0]}{N}$$

□

Cette mesure de confiance dans l'analyse de signature n'a jamais été utilisée à notre connaissance. L'hypothèse de travail retenue par les auteurs dans [Frohwerk 77], [Hassan 84] et [Smith80] est l'équiprobabilité de toutes les réponses fausses. Cette hypothèse n'a aucun sens physique. En effet lorsque la séquence S est appliquée, et compte tenu de l'ensemble de fautes prescrit, toutes les séquences de sortie ne peuvent pas être obtenues. La mesure que nous proposons suppose l'équiprobabilité des réponses fausses possibles.

Définition 5.11 : La **probabilité minimum de non-masquage** notée $\mathbf{P_{Am}}$, est la probabilité minimum de ne pas masquer une réponse fausse.

$$P_{Am} = \min (Pr [A_1 \neq A_0 / Z_1 \neq Z_0], ..., Pr [A_M \neq A_0 / Z_M \neq Z_0])$$

□

Propriété 5.4 : Pour tout circuit, pour tout ensemble de fautes, pour tout analyseur de signature, on a :

$$*P_m \geq P_m P_{Am}$$

Démonstration : Soit f_1 la faute la plus difficile à tester et f_2 la faute la plus difficile à détecter. On a :

$$\forall\ i = 1, ..., M,\quad P_m = Pr [Z_1 \neq Z_0] \leq Pr [Z_i \neq Z_0]$$

$$\forall\ i = 1, ..., M,\quad P_{Am} = Pr [A_2 \neq A_0 / Z_2 \neq Z_0] \leq Pr [A_i \neq A_0 / Z_i \neq Z_0]$$

On a de plus :

$$*P_m = \min (Pr [A_1 \neq A_0], ..., Pr [A_M \neq A_0])$$

Pour tout i = 1, ..., M, on a :

$$Pr [A_i \neq A_0] = Pr [Z_i \neq Z_0] Pr [A_i \neq A_0 / Z_i \neq Z_0]$$
$$\geq P_m P_{Am}$$

□

Définition 5.12 : La **couverture des réponses fausses** notée $\mathbf{P_{Aa}}$, est la probabilité que l'analyseur de signature détecte une réponse fausse.

$$P_{Aa} = Pr [A \neq A_0 / Z \neq Z_0]$$

□

Propriété 5.5 : La couverture des réponses fausses s'écrit :

$$P_{Aa} = Pr [A_1 \neq A_0 / Z_1 \neq Z_0] Pr [f_1/F] + ... + Pr [A_M \neq A_0 / Z_M \neq Z_0] Pr [f_M/F]$$

Démonstration : Les fautes $f_1, ..., f_M$ constituent un ensemble complet d'événements sur F, c'est-à-dire que lorsque $Z \neq Z_0$ une faute et une seule de F est présente dans le circuit sous test. On peut donc écrire :

$$P_{Aa} = Pr [A \neq A_0 / Z \neq Z_0]$$
$$= Pr [(A \neq A_0 / Z \neq Z_0) / f_1] Pr [f_1/F] + ... + Pr [(A \neq A_0 / Z \neq Z_0) / f_M] Pr [f_M/F]$$

Ce qui peut s'écrire de la façon suivante à partir des notations utilisées :

$$P_{Aa} = Pr [A_1 \neq A_0 / Z_1 \neq Z_0] Pr [f_1/F] + ... + Pr [A_M \neq A_0 / Z_M \neq Z_0] Pr [f_M/F]$$

□

Remarques 5.2: 1) La couverture des réponses fausses par l'analyseur de signature est la seule

mesure qui permette de représenter le cas où les fautes qui peuvent se produire sont équiprobables. En effet ce cas ne correspond pas à l'équiprobabilité des réponses fausses.

2) La couverture des réponses fausses est la mesure implicitement utilisée dans la littérature, si toutes les réponses fausses possibles peuvent être obtenues. Le profil d'occurrence des fautes qui conduit à l'équiprobabilité des réponses fausses demande une analyse des fautes pour être calculé.

□

Ces différentes mesures permettent d'estimer la confiance dans l'analyseur de signature, et en particulier de montrer que l'analyse de signature est beaucoup plus performante que la séquence de test en général.

Le problème de masquage lié à cette analyse de signature a été abordé par différents auteurs selon trois approches différentes [David 85]. Dans la première approche ([Frohwerk77]) toutes les séquences de sortie sont supposées équiprobables. La probabilité de masquage d'un circuit défectueux est égale à 2^{-k} si k est le nombre de bascules de la signature. Cette approximation est très optimiste, on s'en rapproche lorsque la longueur de test est très grande. La seconde approche, développée en particulier dans [Smith 80], consiste à étudier certains rebouclages pour certains types d'erreurs. La troisième approche, développée dans [David 80 et 87] [Williams 86], est probabiliste. Les séquences de sortie ne sont pas supposées équiprobables.

Soit $Q_A(f_i)$ la **probabilité de masquer** la faute f_i si elle est présente dans le CST et qu'elle a été testée ($Z_i \neq Z_0$) :

$$Q_A(f_i) = 1 - P_A(f_i) = Pr[A_i = A_0 / Z_i \neq Z_0] \qquad (5.8)$$

On peut écrire par ailleurs :

$$Pr[A_i = A_0] = Pr[A_i = A_0 / Z_i = Z_0]\, Pr[Z_i = Z_0] + Pr[A_i = A_0 / Z_i \neq Z_0]\, Pr[Z_i \neq Z_0]$$
$$= Pr[Z_i = Z_0] + Pr[A_i = A_0 / Z_i \neq Z_0]\, Pr[Z_i \neq Z_0]$$

car l'analyseur de signature ne peut refuser une réponse correcte.

D'où :

$$Q_A(f_i) = \frac{Pr[A_i = A_0] - Pr[Z_i = Z_0]}{Pr[Z_i \neq Z_0]} \qquad (5.9)$$

Soit d_i la probabilité d'un bit de la réponse d'être faux si la faute f_i est présente (d_i est la probabilité de test par un vecteur de la faute f_i). Soient k le nombre de bascules du registre et L la longueur de test. On a alors [David 87] pour un registre rebouclé (seule la sortie de la dernière bascule est ramenée en entrée du registre) :

$$Q_A(f_i) = \frac{2^{-k}(1 + (1 - 2d_i)^a)^b(1 + (1 - 2d_i)^{a+1})^{k-b} - (1 - d_i)^L}{1 - (1 - d_i)^L} \qquad (5.10)$$

avec $a = \left\lfloor \frac{L}{k} \right\rfloor$ et $b = k(a+1) - L$

Remarque 5.3 : Dans [Williams 86] les auteurs étudient la probabilité de masquage en supposant que toutes les réponses sont fausses. Ils définissent alors la probabilité de masquage P_{al} par :

$$P_{al} = Pr[A = A_0] - Pr[Z = Z_0]$$
$$= Pr[A = A_0 \text{ et } Z \neq Z_0]$$

□

Reprenons l'exemple du circuit à 10 entrées, 4 sorties et testé par une séquence de 500 vecteurs aléatoires présenté dans l'introduction de ce chapitre. Soit le test aléatoire compact de ce circuit à l'aide d'un registre à décalage rebouclé comportant 30 bascules. La probabilité de test de la faute f_1 s'écrit :

$$P_T(f_1) = 1 - \left(1 - \frac{10}{1024}\right)^L = 0{,}9926$$

Pour la faute f_1 on peut calculer, à partir des équations 5.8 et 5.10, la probabilité de non-masquage :

$$P_A(f_1) = 0{,}9966$$

L'analyse de signature est donc plus performante que la génération des vecteurs de test. Cette propriété est d'autant plus intéressante que la confiance dans l'analyseur de signature augmente sensiblement quand le nombre de bascules du registre augmente. Pour L = 500 et **k = 50** on a $\mathbf{P_A(f_1) = 0{,}9982}$ alors que $P_T(f_1) = 0{,}9926$.

L'analyseur de signature n'est pas l'élément du dispositif de test qui détermine la confiance dans le test. Ceci est d'autant plus vrai qu'il suffit de rajouter quelques bascules au registre pour rendre l'analyse de signature aussi performante que l'on veut. C'est pourquoi nous ne développerons pas une méthode approchée d'estimation de la couverture des réponses fausses. La définition de la probabilité minimum pondérée de détection relative à une partition de l'ensemble d'erreurs prescrit ne pose aucun problème théorique mais est tout à fait dénué d'intérêt pratique.

b - Relation avec la confiance dans la méthode de test

Revenons un peu en arrière pour voir comment la mesure de la confiance dans l'analyse de signature permet d'approcher $*P_a$, la couverture des circuits défectueux après signature. Pour obtenir $*P_a$ il faut connaître les probabilités de détection et d'occurrence de chaque faute de F. La première approximation que nous avons présentée au paragraphe 5.2.4 permet d'estimer $*P_a$ à

partir des seules fautes les plus difficiles à détecter.

La *seconde approche* que nous proposons ici consiste à minorer la confiance dans la méthode de test à partir du *produit* d'une mesure de confiance dans la séquence de test et d'une mesure de confiance dans l'analyseur de signature.

Bien que la probabilité de détecter une faute f_i soit le produit des probabilités de test et de non -masquage de cette faute on ne peut pas étendre cette propriété aux mesures de la confiance dans la méthode de test. En particulier la couverture des circuits défectueux après signature n'est pas le produit de la couverture des circuits défectueux et de la couverture des réponses fausses.

$$*P_a \neq P_a P_{Aa}$$

Néanmoins on peut minorer cette probabilité à partir des performances de la séquence de test d'une part et de l'analyseur de signature d'autre part .

Théorème 5.5 : Si la génération des vecteurs de test est indépendante de l'analyse de signature alors :

$$*P_a \geq P_a P_{Am}$$

Démonstration : Supposons que la réponse la plus difficile à ne pas masquer soit Z_1. On a alors:

$$P_{Am} = Pr\,[A_1 \neq A_0 / Z_1 \neq Z_0] = P_A\,(f_1)$$

et $\quad \forall\ i = 1, ..., M, \quad P_A\,(f_i) \geq P_A\,(f_1)$

De plus on a $\quad \forall\ i = 1, ..., M, \quad Pr\,[A_i \neq A_0] = Pr\,[A_i \neq A_0 / Z_i \neq Z_0]\ Pr\,[Z_i \neq Z_0]$

D'où $\quad \forall\ i = 1, ..., M, \quad Pr\,[A_i \neq A_0] \geq P_A\,(f_1)\ Pr\,[Z_i \neq Z_0]$

A partir de l'équation (5.4) on a :

$$\begin{aligned} *P_a &= Pr\,[A_1 \neq A_0]\ Pr\,[f_1/F] + ... + Pr\,[A_M \neq A_0]\ Pr\,[f_M/F] \\ &\geq P_A\,(f_1)\ Pr\,[Z_1 \neq Z_0]\ Pr\,[f_1/F] + ... + P_A\,(f_1)\ Pr\,[Z_M \neq Z_0]\ Pr\,[f_M/F] \\ &\geq P_A\,(f_1)\ (Pr\,[Z_1 \neq Z_0]\ Pr\,[f_1/F] + ... + Pr\,[Z_M \neq Z_0]\ Pr\,[f_M/F]) = P_{Am}\ P_a \end{aligned}$$

□

Ce résultat est très intéressant d'un point de vue pratique. En effet P_{Am} peut être très peu différent de 1 si l'analyseur de signature est un registre à décalage à rebouclage linéaire comportant un nombre suffisant d'étages. La couverture des circuits défectueux après signature $*P_a$ peut donc être très proche de la couverture des circuits défectueux P_a. De même $*C_t$ et $*C_a$ peuvent être très proches de C_t et C_a respectivement. Ce théorème nous permet donc de conclure qu'en pratique l*a couverture des circutis défectueux après signature est limitée par le test du circuit mais pas par l'analyse de signature.*

Remarque 5.4 : On peut utiliser conjointement les deux approches proposées pour estimer la

couverture des circuits défectueux après signature. Après avoir estimé la confiance dans l'analyseur de signature à l'aide de la probabilité minimum de non-masquage on peut estimer la couverture des circuits défectueux à l'aide de la probabilité minimum pondérée de test. Soit la relation :

$$*P_a \geq P_a\, P_{Am} \geq P_w(\rho)\, P_{Am}$$

Lorsque la longueur de test est petite, P_{Am} est une estimation trop grossière de la confiance dans l'analyseur de signature. On peut alors estimer la couverture des circuits défectueux après signature à partir de la probabilité minimum pondérée de détection et de la propriété 5.4. On a alors :

$$*P_a \geq *P_w(\rho) \geq Pr[F_1/F]\, P_m(F_1)\, P_{Am}(F_1) + \ldots + Pr[F_r/F]\, P_m(F_r)\, P_{Am}(F_r)$$

□

5 .4 . Test compact statistique

Le test aléatoire d'un circuit consiste à appliquer à ce circuit une séquence de test dont on ne connait que les propriétés statistiques. Cette séquence n'est, en général, pas reproductible (on peut assimiler une séquence aléatoire préenregistrée à une séquence pseudo-aléatoire). Si on effectue k expériences de test sur un même circuit (on applique k séquences aléatoires avec les mêmes propriétés statistiques), on obtient k réponses différentes en général. Ceci est vrai en particulier pour un circuit sans faute. Il n'existe donc pas de réponse Z_0 de référence mais autant de réponses correctes que de séquences de test différentes. Toutefois les propriétés statistiques de la réponse correcte sont connues à partir des propriétés statistiques de la séquence de test [Parker 76]. Ces propriétés sont une image compacte de la réponse : on parle de **test compact statistique.**

Soit le test aléatoire d'une porte ET à deux entrées. L'image de la réponse est le nombre moyen de 1 qu'elle contient. Si les vecteurs d'entrée sont équiprobables la probabilité de 1 en sortie d'un circuit sans faute est égale à 0,25. Cette probabilité est réalisée pour une longueur de test infinie. Au cours d'une expérience de test, c'est-à-dire la réalisation d'une séquence aléatoire de longueur L, on n'a pas exactement le quart des bits de sortie égaux à 1. Les deux expériences de test décrites à la figure 5.12 le montrent.

Pour une séquence aléatoire de longueur 10 il y a en moyenne 2,5 bits de sortie égaux à 1. On peut donc admettre que les circuits dont la réponse contient 2 ou 3 bits égaux à 1 sont sans faute. De façon plus générale on se donne un *intervalle de confiance* dans lequel on considère que le circuit est sans faute. Pour notre exemple on peut choisir comme règles de décision :

1) si $0{,}2 \leq \frac{A}{L} \leq 0{,}3$ alors le circuit est sans faute

sinon 2) le circuit est défectueux

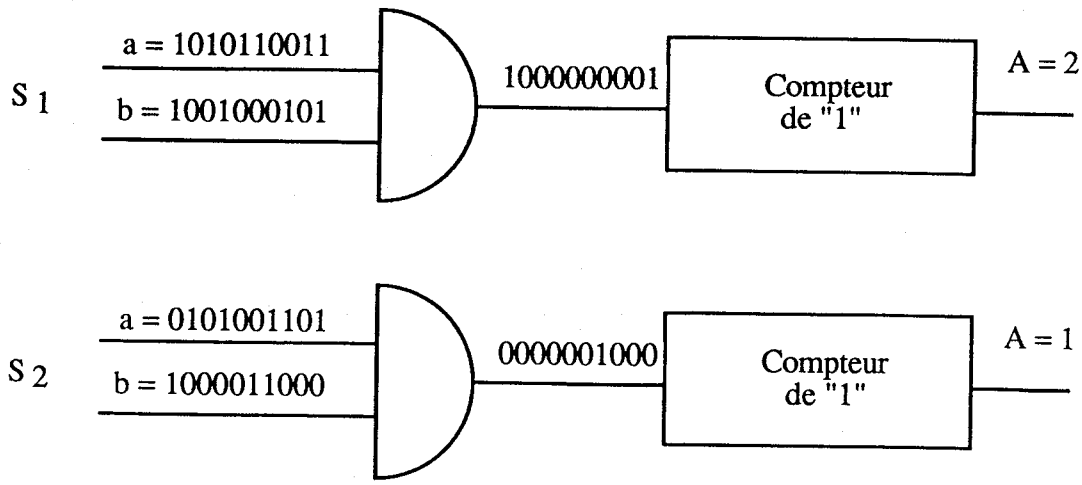


Figure 5.12 : Deux expériences de test compact statistique

On n'a plus une signature correcte A_0 mais un *ensemble de signatures admises* que l'on note A_0^+. Cet ensemble est défini par l'intervalle de confiance que l'on c'est donné. Dans l'exemple précédent on a :

$$A_0^+ = \{ A / 0{,}2 \leq \frac{A}{L} \leq 0{,}3 \}$$

Donc si L = 10 on $A_0^+ = \{2, 3\}$ puisque A est un nombre entier.

Avec ces règles de décision une porte sans faute testée avec la séquence S_1 (figure 5.12) est correctement testée, alors qu'une porte sans faute testée avec la séquence S_2 est refusée.

Le test compact statistique ne répond donc pas au schéma de test que nous avons étudié jusque là puisqu'*un circuit sans faute peut être refusé.*

Propriété 5.6 : La probabilité de détection d'une faute f_i s'écrit :

a) $P_D(f_0) = Pr[A_0 \in A_0^+]$

b) $P_D(f_i) = Pr[A_i \notin A_0^+]$ pour i = 1, ..., M

Démonstration : a) Si la faute f_0 est présente dans le circuit sous test ce circuit est sans faute. Le résultat de la détection est juste si le circuit est reconnu bon, c'est-à-dire si sa signature appartient à l'ensemble de signatures admises.

b) Si la faute f_i, $i \neq 0$, est présente dans le circuit sous test le résultat de la détection est juste si une erreur apparaît dans la signature du circuit lorsque f_i est présente. On a donc :

$$P_D(f_i) = Pr[A \notin A_0^+/f_i] = Pr[A_i \notin A_0^+]$$

□

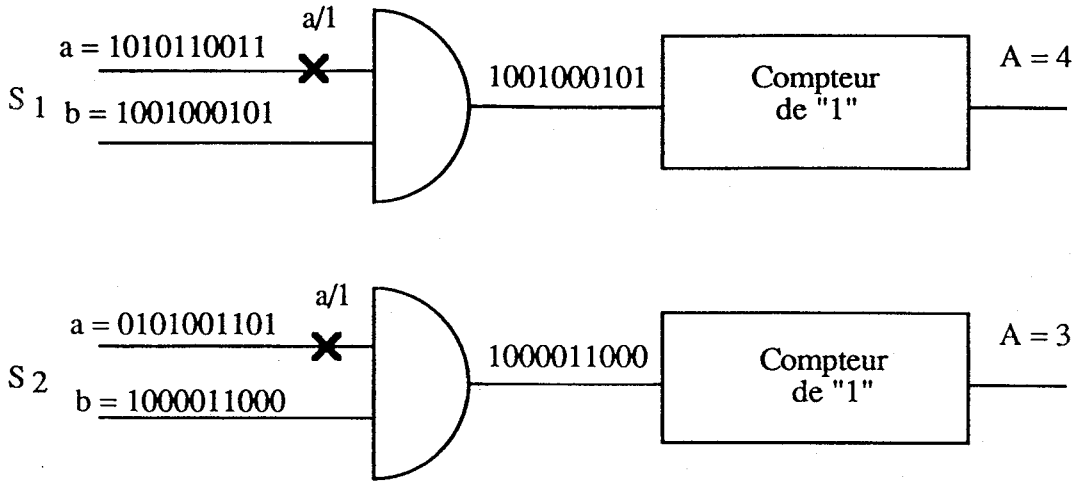


Figure 5.13 : Test compact statistisque d'une porte défectueuse

Supposons maintenant que la porte ET testée soit affectée de la faute f_1 qui est le collage à 1 de l'entrée "a". La figure 5.13 décrit le test de cette porte par les séquences S_1 et S_2. Une porte ET affectée de la faute f_1 est refusée si la séquence S_1 est appliquée mais elle est masquée si la séquence S_2 est appliquée.

Pour un ensemble de circuits testés avec une méthode de test compact statistique deux types d'erreur de test peuvent se produire : certains circuits défectueux passent le test et certains circuits sans faute sont refusés (figure 5.14). Le cas du test compact statistique diffère de l'analyse de signature avant tout parce que tous les circuits sans faute ne passent pas le test. De ce fait les mesures de la confiance dans les circuits testés après signature s'écrivent en fonction de la probabilité qu'une réponse correcte conduise à une image fausse. Les définitions de la confiance moyenne dans les circuits testés après signature $*C_t$ et de la confiance moyenne dans les circuits passés après signature $*C_a$ sont les même que pour l'analyse de signature mais les propriétés qui en découlent diffèrent. On a :

$$*C_t = Pr [f_0 \text{ et } A \in A_0^+] + Pr [F \text{ et } A \notin A_0^+]$$

A_0^+ représente l'ensemble des images compactes des circuits qui sont reconnus sans faute à partir des règles de décision. On peut aussi écrire :

$$*C_t = Pr [f_0] \, Pr [A \in A_0^+ / f_0] + Pr [F] \, Pr [A \notin A_0^+ / F]$$

A partir de la définition 5.2 on écrit la propriété 5.7.

Propriété 5.7: Pour tout circuit, pour tout ensemble de fautes, pour tout test compact statistique, la confiance moyenne dans les circuits testés après signature s'écrit :

$$*C_t = Y \, Pr [A \in A_0^+ / f_0] + (1 - Y) \, *P_a \qquad (5.11)$$

□

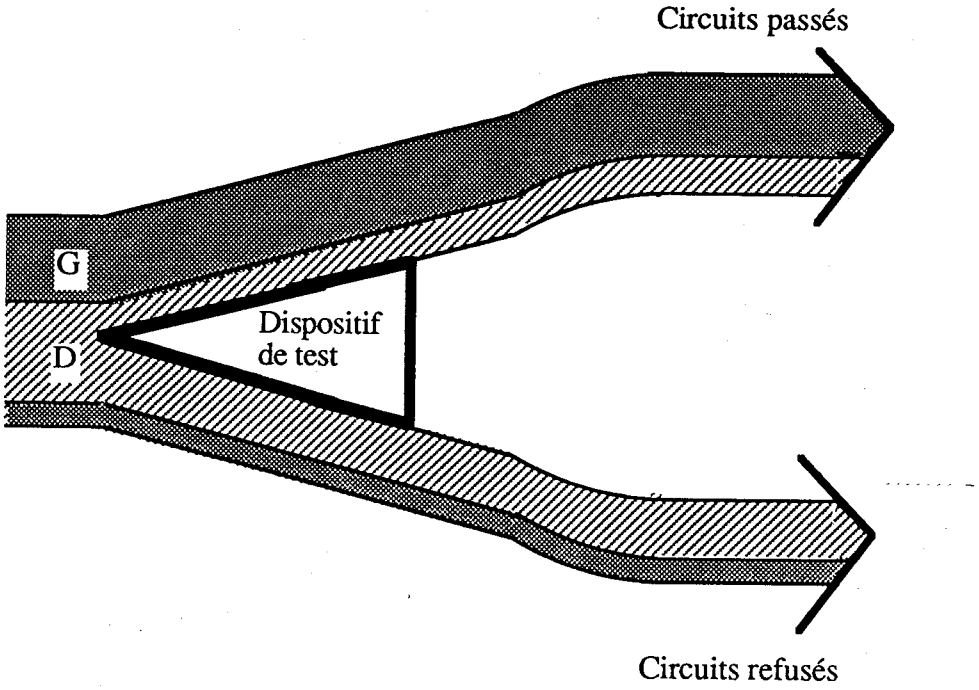


Figure 5.14 : Test compact statistique

Remarque 5.5 : Le terme Pr [A ∈ A_0^+ / f_0] est la probabilité qu'un circuit sans faute soit passé. Dans le cadre de notre étude cette probabilité caractérise la capacité du dispositif d'observation de la réponse du CST à reconnaître un circuit sans faute. Dans le cas plus général où le dispositif de test peut être défectueux Pr [A ∈ A_0^+ / f_0] représente la probabilité que le dispositif de test n'introduise pas d'erreur quelle que soit la méthode de test utilisée.

L'hypothèse retenue dans tous les travaux est que la dispositif de test est beaucoup plus fiable que le circuit à tester. Cette hypothèse n'est pas réellement justifiée pour les circuits avec test intégré. Dans ce cas le résultat du test doit porter sur tout le composant (dispositif de test compris) qui est dans sa totalité utilisé ou détruit. On ne peut plus distinguer le dispositif de test du circuit et les fautes qui peuvent l'affecter doivent être dans l'ensemble de fautes prescrit. Compte tenu de cette remarque nous n'avons pas développé cet aspect. Toutefois les résultats obtenus dans cette partie consacrée au test compact statistique peuvent être appliqués si le dispositif de test est défectueux.

□

A partir de la définition 5.3 on peut écrire la confiance moyenne dans les circuits passés après signature en fonction de *P_a et Y.

Propriété 5.8 : Pour tout circuit, pour tout ensemble de fautes, pour tout test compact statistique

la confiance moyenne dans les circuits passés après signature s'écrit :

$$*C_a = \frac{Y \Pr[A \in A_0^+ / f_0]}{Y \Pr[A \in A_0^+ / f_0] + (1 - Y)(1 - *P_a)} \qquad (5.12)$$

Démonstration : La définition 5.3 s'écrit :

$$*C_a = \Pr[f_0 / A \in A_0^+]$$

On peut écrire de plus :

$$\Pr[f_0] = \Pr[f_0 / A \in A_0^+] \Pr[A \in A_0^+] + \Pr[f_0 / A \notin A_0^+] \Pr[A \notin A_0^+]$$

On obtient alors :

$$*C_a = \frac{\Pr[f_0] - \Pr[A \notin A_0^+] \Pr[f_0 / A \notin A_0^+]}{\Pr[A \in A_0^+]}$$

$$\Pr[A \notin A_0^+] \Pr[f_0 / A \notin A_0^+] = \Pr[f_0 \text{ et } A \notin A_0^+] = \Pr[f_0] \Pr[A \notin A_0^+ / f_0]$$
$$= Y (1 - \Pr[A \in A_0^+ / f_0])$$

$$\Pr[A \in A_0^+] = \Pr[f_0] \Pr[A \in A_0^+ / f_0] + \Pr[F] \Pr[A \in A_0^+ / F]$$
$$= Y \Pr[A \in A_0^+ / f_0] + (1 - Y)(1 - *P_a)$$

□

Propriété 5.9 : Pour tout circuit, pour tout ensemble de fautes et pour tout test compact statistique la confiance moyenne dans les circuits testés $*C_t$ et la confiance moyenne dans les circuits passés $*C_a$ sont des fonctions croissantes de $*P_a$ pour tout Y tel que $0 < Y < 1$ et pour tout $0 < \Pr[A \in A_0^+ / f_0]$.

Démonstration : Afin d'alléger les notations on notera $p = \Pr[A \in A_0^+ / f_0]$. On a :

$$*C_t = Y p + (1 - Y) *P_a$$

$$*C_a = \frac{Y p}{Y p + (1 - Y)(1 - *P_a)}$$

D'où on calcule :

$$\frac{d *C_t}{d *P_a} = (1 - Y) \geq 0$$

$$\frac{d*C_a}{d*P_a} = \frac{(1 - Y) Y p}{(Yp + (1 - Y)(1 - *P_a))^2} \geq 0$$

□

Dans le cas du test compact statistique il n'existe pas de relation d'ordre entre $*C_t$ et $*C_a$ car les circuits refusés ne sont pas tous correctement testés. Il n'existe pas non plus de relation d'ordre entre $*C_t$ et $*P_a$. A partir de l'équation (5.11) on peut calculer :

$$*C_t - *P_a = Y\ (Pr\ [A \in A_0^+ / f_0] - *P_a)$$

Si la probabilité d'obtenir un résultat juste pour un circuit sans faute est supérieure à la probabilité de détecter un circuit défectueux alors $*C_t \geq *P_a$. Cette condition n'est pas très restrictive en pratique.

Les mesures de la confiance dans la méthode de test telles que nous les avons définies dans la partie 5.2 caractérisent la capacité de la méthode de test à détecter un circuit défectueux. Ces mesures ne tiennent pas compte des circuits sans faute. Aussi les théorèmes 5.2 et 5.3 ainsi que le corollaire 5.1 sont vrais pour un test compact statistique.

Par contre il n'existe pas de relation d'ordre entre $Pr\ [A \notin A_0^+]$ et $Pr\ [Z \neq Z_0]$ car l'événement $A \notin A_0^+$ peut se produire sans que l'événement $Z \neq Z_0$ se soit produit. Le théorème 5.4 n'est donc plus vrai.

On peut s'interroger sur la signification des mesures de la confiance dans la méthode de test lorsque celle ci est imparfaite pour tester à la fois les circuits défectueux et les circuits sans faute. La confiance dans la méthode de test doit tenir compte de tous les circuits testés. On peut définir des extensions des définitions 5.4 à 5.6 en considérant l'ensemble de fautes prescrit suivant :

$$F' = \{f_0, f_1, ..., f_M\}$$

En ce qui concerne la couverture des réponses fausses $*P_a$ son extension à l'ensemble des circuits testés conduit à la confiance moyenne dans les circuits testés comme nous l'avons déjà souligné à la remarque 3.5. Ceci justifie, s'il était nécessaire, le choix de $*P_a$ comme étant la mesure la plus significative de la confiance dans la méthode de test.

L'étude de la confiance dans un test que nous avons développée dans ce chapitre, a permis de montrer que l'analyse de signature ne limite pas la performance d'un test. En effet :

1) plusieurs méthodes de construction d'une séquence de test déterministe ont été développées. Ces méthodes permettent d'obtenir une couverture complète de l'ensemble de fautes prescrit lorsqu'une méthode de comptage est utilisée pour observer la réponse du circuit sous test.

2) lorsque la séquence de test est pseudo-aléatoire, la confiance dans la méthode de test peut être aussi proche que l'on veut de la confiance dans la séquence de test, si on utilise pour compacter la réponse du circuit sous test un registre à décalage à rebouclage linéaire. Toutefois si on veut optimiser le nombre de bascules du registre de signature il faut connaître l'influence des paramètres suivants sur la probabilité de masquage d'une faute : la probabilité de test de cette faute, la longueur de test et le nombre de bascules du registre. L'étude développée dans la chapitre 7 met en évidence, sur un exemple, les problèmes qui peuvent se poser.

Le formalisme qui a été développé dans les chapitres précedents à partir de la réponse du circuit sous test peut être intégralement repris à partir de la signature du circuit. L'analyse de signature entraine une perte de confiance ; par analogie avec la séquence de test on mesure la capacité de l'analyseur de signature à ne pas masquer une réponse fausse. Si par contre l'image compacte de la réponse du circuit sous test n'est pas entièrement connue (test compact statistique) on ne peut pas dissocier du point de vue de la mesure de confiance le test par la séquence de test du non-masquage par l'observateur. Dans ce cas les mesures développées jusque là s'écrivent de façon différente en fonction du rendement de fabrication et de la capacité du dispositif de test à détecter un circuit défectueux. De fait il existe peu de relations formelles entre ces mesures.

Partie B

Application

Chapitre 6

Test des circuits CMOS

Nous avons appliqué les différents résultats obtenus dans la partie précédente à un microprocesseur réalisé en technologie CMOS. Après une brève description de la technologie, ses problèmes spécifiques de test sont décrits. Les fautes de transistor collé ouvert, qui sont les plus difficiles à tester, sont plus particulièrement étudiées.

6 . 1 . Introduction

Dans le domaine de l'électronique l'enjeu est le suivant : il s'agit d'effectuer un maximum d'opérations logiques dans des conditions optimales de fiabilité et dans l'espace le plus réduit possible. Le maître mot est *miniaturisation.* Au cours de ces 20 dernières années le nombre de transistors par puce a doublé tous les quinze mois. Néanmoins certaines contraintes physiques limitent cette marche à l'intégration massive. La dissipation d'énergie dans des espaces de plus en plus réduits est l'une de ces contraintes. Un des très grands avantages de la technologie CMOS (Complementary Metal Oxyde Semiconductor) est sa faible consommation statique. C'est la raison pour laquelle ces composants sont omniprésents dans la microéléctronique "grand-public". Les circuits actuels sont réalisés en couplant des milliers, voire des millions, de composants CMOS sur une même puce.

Dans un circuit CMOS certaines défaillances entrainent des mauvais fonctionnements qui sont liés à la technologie. En effet il existe deux modèles de fautes propres aux circuits CMOS : les *collages ouverts* (ou *S-open*) et les *collages fermés* (ou *S-on.*). Ces deux fautes sont relatives à un transistor alors que les modèles de fautes valables pour toutes les technologies sont définies au niveau des portes logiques [Galiay 80].

Remarque 6.1 : L'effet thyristor, ou **latch-up**, est une défaillance propre aux circuits CMOS. Ce phénomène conduit à des fautes qui évoluent dans le temps. Certaines règles de conception d'un circuit CMOS permettent de limiter sa sensibilité au latch-up [Genda 84], c'est pourquoi nous n'étudierons pas cette faute.

□

Les transistors collés ouverts sont des fautes particulièrement difficiles à tester car elles *transforment* un circuit combinatoire en un circuit *séquentiel* [Wadsack 78]. L'étude du test des transistors collés ouverts qui a été développée jusque là ([Elziq 81] [Chandramouli 83] [Baschiera 84] [Darlay 88]), a conduit au résultat suivant : pour tester un transistor collé ouvert il faut appliquer en entrée de la porte défectueuse une **séquence de deux vecteurs de test.**

Certaines fautes de transistors collés ouverts sont équivalentes au collage classique à 1 ou à 0 de la sortie de la porte défectueuse. Ces fautes sont testées par un **vecteur d'entrée** et non pas par une séquence. Elles ne sont donc pas particulièrement difficiles à tester. On parlera de la *sensibilité d'un transistor à une faute de collage ouvert.*

En présence de certaines fautes un circuit CMOS perd sa propriété de ne pas consommer de courant en dehors des instants de commutation. La mesure de courant est une méthode très utilisée pour tester les courts-circuits [Acken 83] et les collages fermés [Baschiera 84]. Nous verrons qu'elle peut également permettre de détecter des collages ouverts qui ne sont pas testés par un test logique.

L'étude que nous avons développée dans la partie A a mis en évidence le fait que deux paramètres caractérisent une faute : sa probabilité de test et sa probabilité d'occurrence. Après avoir détaillé le test des fautes les plus difficiles à tester dans un circuit CMOS, nous étudierons les hypothèses qui permettent d'estimer la probabilité d'occurrence d'une faute de transistor collé ouvert.

6 . 2 . Description de la technologie CMOS

Le transistor métal oxyde silicium (ou MOSFET) est l'élément de base des circuits intégrés d'aujourd'hui. On dit qu'il est à **effet de champ** car c'est un champ électrique qui module le débit du courant électrique.

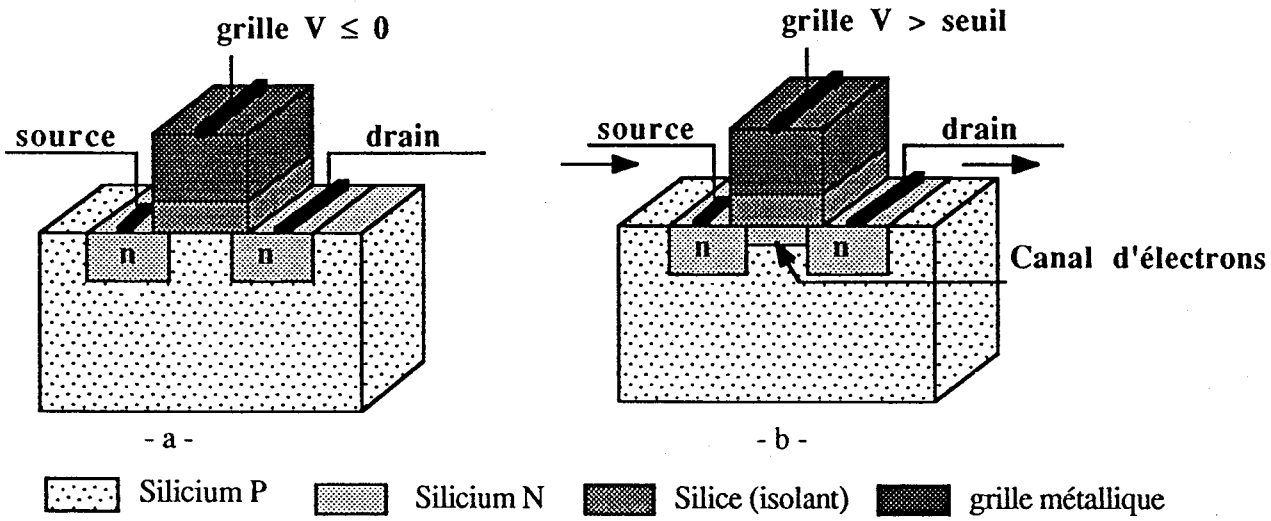


Figure 6.1 : Description d'un transistor MOS
a - Transistor N bloqué b - Transistor N passant

Le **MOSFET** de type N est constitué d'un cristal de silicium *déficitaire* en électrons

dans lequel sont introduites deux régions, le **drain** et la **source**, *riches* en électrons. Le fonctionnement du transistor est controlé par une électrode métallique, la **grille**, qu'une couche d'oxyde isole électriquement du silicium (figure 6.1a). Lorsqu'un potentiel électrique négatif ou nul est appliqué à la grille les électrons sont chassés dans le corps du silicium et aucun courant ne passe entre le drain et la source : le transistor est **bloqué**. Lorsqu'une tension positive suffisament élevée est appliquée à la grille les électrons sont attirés à l'interface silicium silice et forment un canal conducteur entre le drain et la source. Le transistor est **passant** (figure 6.1b).

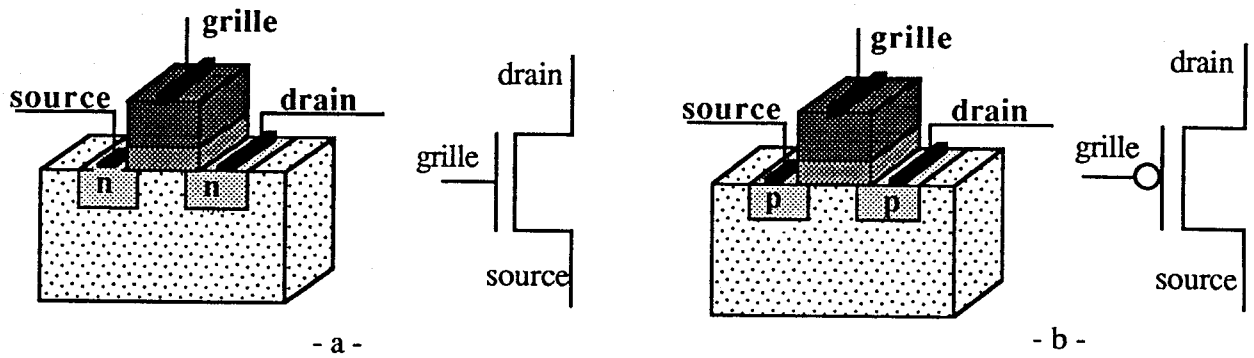


Figure 6.2 : Représentation symbolique
a - Transistor N b - Transistor P

Une porte logique CMOS réunit les deux types de MOSFET : les transistors de type N et les transistors de type P. Le type (N ou P) du transistor fait référence à la polarité des porteurs dans le canal, polarité qui est la même que celle du drain et de la source. Dans le cas d'un transistor de type P dont les porteurs sont des trous il faut que la tension de la grille soit négative pour attirer les trous de façon à rendre passant le transistor. La représentation symbolique d'un transistor P et d'un transistor N est donnée à la figure 6.2.

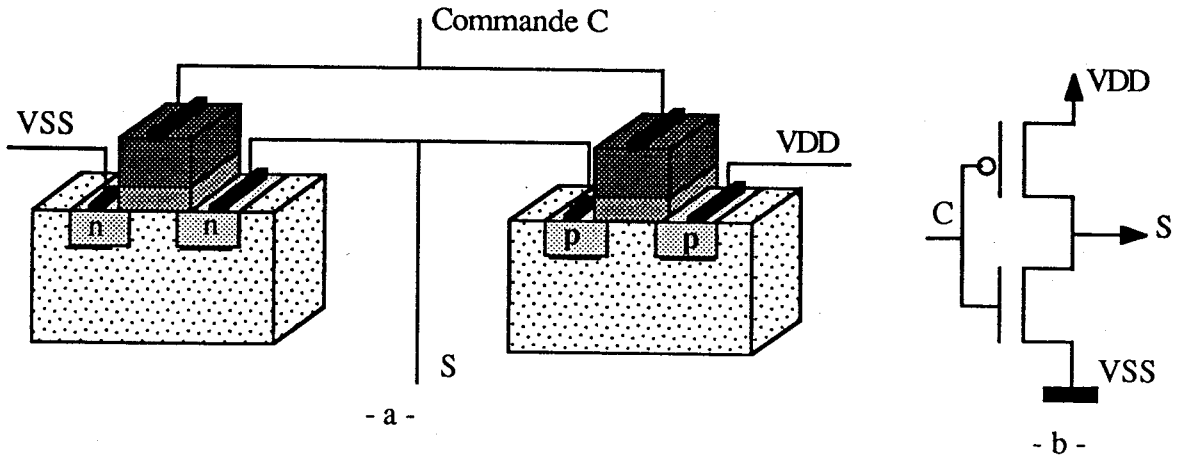


Figure 6.3 : Inverseur CMOS
a - Description technologique b - Représentation symbolique

On notera V_{DD} et V_{SS} la tension d'alimentation (**niveau logique 1**) et la masse

(niveau logique 0) respectivement. Un inverseur CMOS est représenté à la figure 6.3. Lorsque C = 1 le transistor P est bloqué et la sortie est connectée à la masse à travers le transistor N passant, S = 0. Lorsque C = 0 le transistor N est bloqué et la sortie est connectée à l'alimentation à travers le transistor P passant, S = 1. Grâce à l'isolant de la grille aucun courant ne passe entre les deux transistors et la circuit ne consomme pratiquement pas d'énergie quand il ne commute pas.

L'inverseur est la porte **Full-CMOS** la plus simple. Une porte Full-CMOS est composée d'un réseau de transistors P qui relie la sortie à V_{DD} et d'un réseau dual de transistors N qui relie la sortie à V_{SS} (figure 6.4).

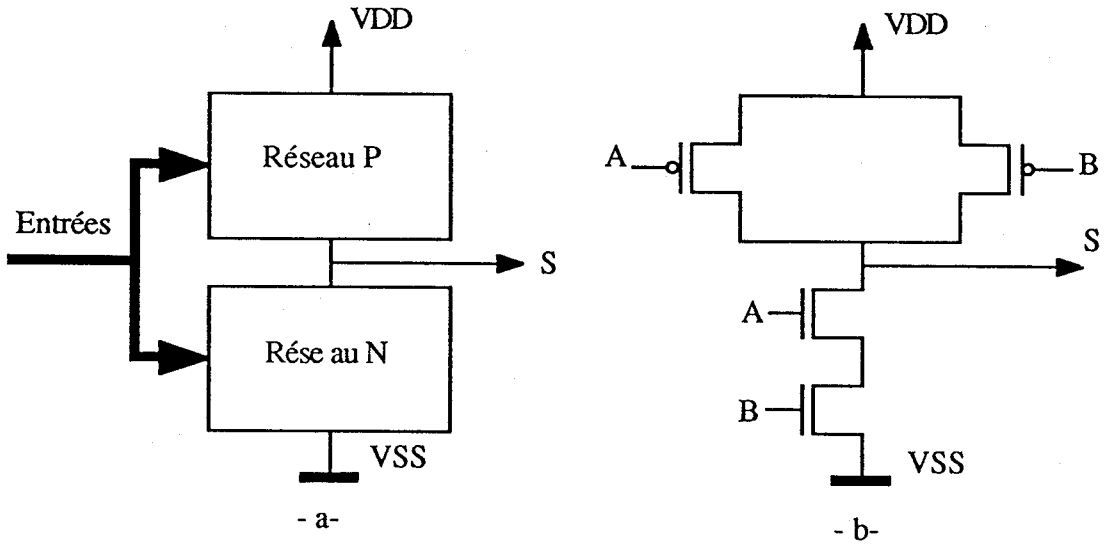


Figure 6.4 : Structure Full-CMOS
a - Structure générale b - Porte Nand

Lorsque le *réseau P* est *passant*, c'est-à-dire qu'il existe un chemin conducteur entre V_{DD} et S, le *réseau N* est *bloqué*, c'est-à-dire qu'il n'existe pas de chemin conducteur entre V_{SS} et S. Réciproquement lorsque le réseau N est passant le réseau P est bloqué. Pour chaque vecteur d'entrée possible soit le réseau P est passant soit le réseau N est passant.

6 . 3 . Modèles de fautes

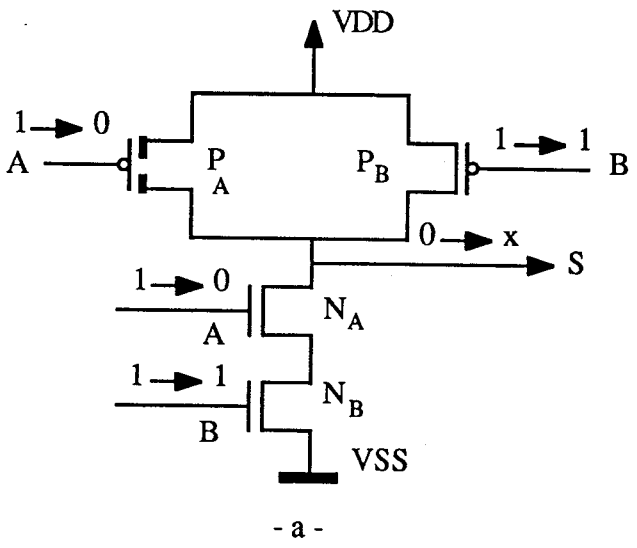
Certains modèles de fautes sont valables pour tous les circuits logiques. C'est le cas des fautes qui sont définies au niveau des portes logiques comme les collages à 1 ou à 0, les courts-circuits entre interconnexions et les retards. Etant donnée une technologie d'autre fautes peuvent également affecter un circuit. Pour la technologie CMOS certaines défaillances au niveau du transistor ne peuvent être modélisées au niveau des portes logiques. Les fautes de transistor

collé ouvert (S-open) et de transistor collé fermé (S-on) sont deux modèles associés à la technologie CMOS.

6 . 3 . 1 . Transistors collés ouverts

Un contact mal pris (grille, drain ou source) ou un canal trop étroit sont des défaillances qui entrainent une faute de **transistor collé ouvert** ou **S-open**. La présence de cette faute dans un circuit CMOS a été mise en évidence par Wadsack [Wadsack 78]. Lorsqu'un transistor est collé ouvert dans une porte Full-CMOS il existe des vecteurs d'entrée pour lesquels ni le réseau P ni le réseau N ne sont passants. Lorsque l'un de ces vecteurs est appliqué en entrée du circuit la sortie de la porte défectueuse entre dans un **état de haute impédance** et conserve la valeur qu'elle avait prise précédemment.

Soit la porte Nand à 2 entrées représentées à la figure 6.5a dans laquelle le transistor P commandé par la variable A est collé ouvert.



- a -

A	B	So	S
0	0	1	1
0	1	1	x
1	1	0	0
1	0	1	1

x valeur précédente

- b -

Figure 6.5 : Test d'un collage ouvert
a - Porte Nand défectueuse b - Vecteurs de test

Lorsque le vecteur AB = 01 est appliqué le transistor N_B est passant, le transistor P_B est bloqué. Le transistor N_A est bloqué ce qui isole la sortie de la masse, et le transistor P_A devrait être passant mais il est ouvert du fait de la faute, la sortie S de la porte défectueuse n'est pas connectée à l'alimentation. Elle garde la valeur X qu'elle avait prise précédemment. Il y a apparition d'un **point mémoire**.

Le test de cette faute est **séquentiel**, il comprend deux phases. Brzozowski dans [Brzozowski 86] parle de *faute dynamique*. Dans un premier temps il faut initialiser le point mémoire et dans un second temps il faut tester l'effet mémoire. Les vecteurs T_1 qui permettent

d'initialiser le point mémoire sont ceux qui mettent la sortie de la porte défectueuse à 0 (respectivement 1) si un transistor P (respectivement N) est collé ouvert. Pour la porte Nand T_1 = AB = 11 est le seul vecteur d'initialisation possible. Les vecteurs T_2 qui permettent de tester l'effet mémoire sont ceux qui mettent la sortie de la porte défectueuse dans un état de haute impédance. Ces vecteurs vérifient les deux propriétés suivantes :

1) le réseau N (respectivement P) est bloqué et le chemin conducteur qui connecte S à l'alimentation (respectivement la masse) est ouvert si le transistor P (respectivement N) testé est collé ouvert.

2) il existe un vecteur T_1 d'initialisation adjacent au vecteur T_2 de test.

Pour la porte Nand T_2 = AB = 01 est le seul vecteur de test possible. Si on applique la séquence T_1T_2 = (11, 01) en entrée de la porte défectueuse de la figure 6.5 on obtient la séquence de sortie S = 00 alors que la séquence de sortie d'une porte sans faute est S_0 = 01.

Nous verrons dans la partie 6.4 consacrée au test des collages ouverts que, d'une part il n'existe pas toujours une séquence T_1T_2 de deux vecteurs adjacents et que, d'autre part toutes les fautes de transistor collé ouvert ne nécessitent pas une séquence de deux vecteurs de test.

6 . 3 . 2 . Transistors collés fermés

Les caractéristiques technologiques (canal étroit) et leurs modifications sont à l'origine d'un **transistor collé fermé** (ou **toujours passant**). Ainsi toute faute qui modifie la tension de seuil ou la conductivité du canal peut engendrer une faute de transistor collé fermé.

Lorsqu'un transistor est toujours passant dans une porte CMOS il existe des vecteurs d'entrée pour lesquels le réseau P et le réseau N sont tous les deux conducteurs. Lorsque l'un de ces vecteurs est appliqué en entrée du circuit il existe un chemin conducteur entre l'alimentation et la masse. La sortie de la porte défectueuse est comprise entre V_{DD} et V_{SS}. Il y a apparition d'une **valeur analogique**. Cette valeur dépend de l'impédance équivalente des chemins conducteurs dans le réseau N et dans le réseau P.

Soit la porte Nand à 2 entrées représentée à la figure 6.6a dans laquelle le transistor P_A est collé fermé. Lorsque le vecteur AB = 11 est appliqué les transistors N_A et N_B sont passants et la sortie est connectée à la masse. Les transistors P_A et P_B devraient être bloqués et ainsi déconnecter la masse de l'alimentation. Mais du fait de la faute le transistor P_A est passant et la sortie est connectée à V_{DD}.

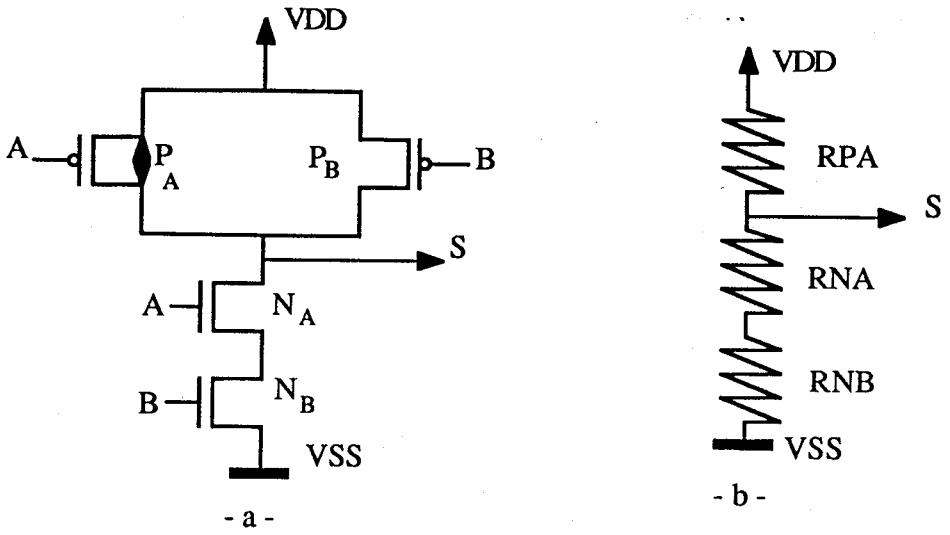


Figure 6.6 : Collage fermé
a - Porte Nand défectueuse b - Réseau résistif équivalent

Le potentiel obtenu en sortie de la porte défectueuse dépend du rapport des impédances des réseaux N et P (figure 6.6b).

$$V_S = V_{DD} \frac{RNA + RNB}{RNA + RNB + RPA}$$

Un vecteur d'entrée permet de détecter un transistor P (resp. N) toujours passant s'il vérifie les propriétés suivantes :

1) pour une porte sans faute le réseau P (resp. N) est bloqué et le réseau N (resp. P) est passant lorsque l'on applique ce vecteur.

2) en présence de la faute il existe un chemin conducteur entre la sortie de la porte défectueuse et V_{DD} (resp. V_{SS}).

Soit la porte décrite à la figure 6.7a dans laquelle le transistor N commandé par la variable A est collé fermé. Les vecteurs de test possibles sont indiqués à la figure 6.7d. A chacun de ces vecteurs correspond un réseau résistif entre V_{DD} et V_{SS}. Les réseaux associés aux vecteurs T_1 et T_2 sont décrits aux figures 6.7b et 6.7c. A partir de ces réseaux et compte tenu des caractéristiques de la technologie, on peut calculer le potentiel de sortie obtenu lorsque chacun de ces vecteurs est appliqué en entrée de la porte défectueuse. Le vecteur T_1 conduit à $V_S = 1{,}5$ V qui est reconnu comme un niveau logique 0 par les portes en aval de la porte défectueuse. Le vecteur T_2 conduit à $V_S = 3$ V qui est reconnu comme un niveau logique 1. Lorsque les vecteurs T_1 et T_2 sont appliqués en entrée d'une porte sans faute la sortie est au niveau logique 1. Le vecteur T_1 permet donc de détecter le transistor toujours passant alors que le vecteur T_2 ne fait pas apparaître d'erreur logique en sortie du circuit.

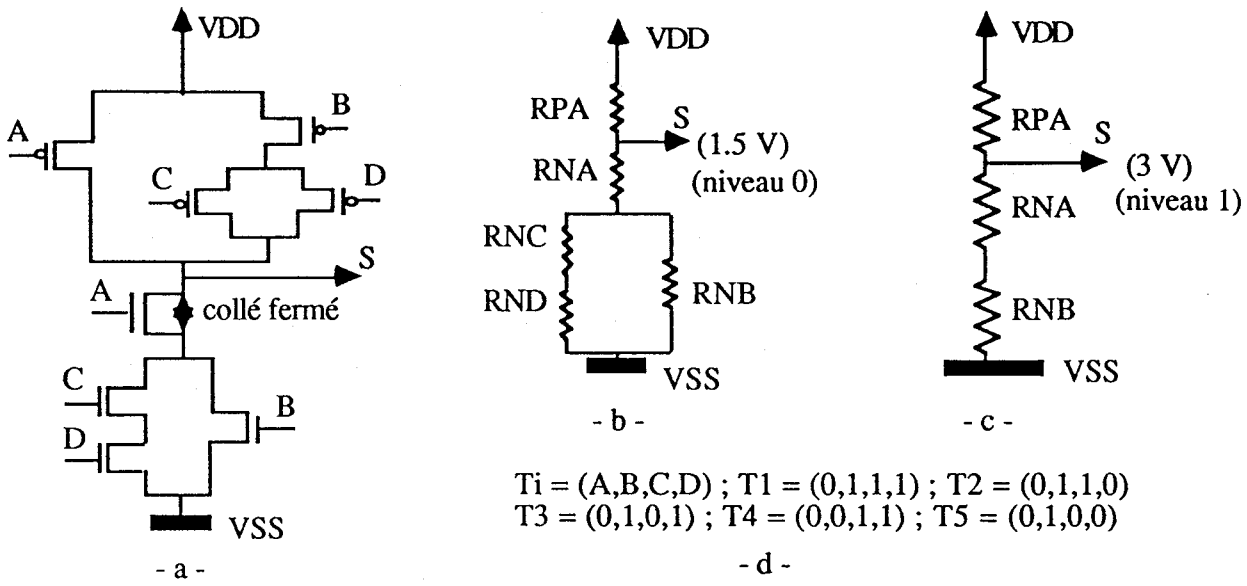


Figure 6.7 : Collage fermé dans une porte Full-CMOS complexe
a - Porte défectueuse b - Réseau résistif équivalent à T1 = (0,1,1,1)
c - Réseau résistif équivalent à T2 = (0,1,1,0) d - Vecteurs de test de la faute.

Cet exemple nous montre que tous les vecteurs de test d'une faute de transistor toujours passant n'introduisent pas d'erreur logique. Le test fonctionnel des transistors collés fermés nécessitent de connaître précisément les caractéristiques électriques du circuit. De nombreuses simulations peuvent être nécessaires pour choisir correctement les vecteurs de test.

Par ailleurs tous les vecteurs qui testent un transistor toujours passant introduisent un chemin conducteur entre V_{DD} et V_{SS} . La mesure de la consommation statique de courant est souvent préconisée comme méthode de test des transistors collés fermés [Baschiera 84]. Brzozowski dans [Brzozowski 86] montre que si on ajoute un transistor et une sortie sur chaque porte Full-CMOS alors aucune faute ne fait apparaître de valeur analogique dans le circuit. Les collages fermés sont testés par une séquence de deux vecteurs. Cette méthode permet d'éviter un test par mesure de courant mais elle est coûteuse en surface de silicium.

Les courts-circuits combinatoires dans les circuits CMOS introduisent également des chemins conducteurs entre V_{DD} et V_{SS} [Acken 83].

6 . 4 . Test des transistors collés ouverts

De manière générale on peut distinguer dans un circuit combinatoire deux types de fautes selon qu'elles introduisent ou non un comportement séquentiel du circuit. Dans les technologies *monocanal* seuls certains courts-circuits entrainent un comportement séquentiel. Le test des collages classiques détecte les courts-circuits qui sont les plus fréquents [Mei 74] ; on

suppose généralement que les autres ne sont pas dans l'ensemble de fautes prescrit. Alors la faute la plus difficile à tester est détectée par au moins un vecteur d'entrée. En technologie CMOS les fautes de transistor collé ouvert entrainent un comportement séquentiel. Il n'est pas réaliste de les ignorer. Aussi la faute la plus difficile à tester est détectée par une séquence de plusieurs vecteurs d'entrée.

Les fautes qui affectent un circuit CMOS peuvent être divisées en 3 classes [Thorel 87a]. La **classe A** regroupe les fautes qui conservent au circuit son caractère combinatoire. Ce sont les collages classiques, les collages fermés et certains courts-circuits. La **classe B** regroupe les fautes qui sont testées par au moins une séquence de deux vecteurs d'entrée. Ce sont la plupart des collages ouverts et certains courts-circuits. La **classe C** regroupe les fautes dites de *séquentialité multiple* pour lesquelles il n'existe pas de séquence de deux vecteurs d'entrée qui les détectent (mais des séquences de test de plus de deux vecteurs d'entrée existent). Ce sont certains collages ouverts et certains courts-circuits. Cette classe ne regroupe qu'un nombre restreint de fautes. En effet nous avons montré [Jacomino 86] que toute faute de transistor collé ouvert dans un circuit de portes Nand (ou Nor) non reconvergent est testée par au moins une séquence de deux vecteurs d'entrée. Seules des portes complexes ou des circuits redondants peuvent être affectés des fautes de la classe C. On peut donc admettre qu'en suivant certaines règles de construction aucune faute de transistor collé ouvert ne nécessite une séquence de test de plus de deux vecteurs d'entrée.

Pour un circuit CMOS l'ensemble de fautes prescrit que nous retiendrons sera constitué de toutes les fautes appartenant à la classe A et à la classe B. Dans cet ensemble la faute la plus difficile à tester est *à priori* une faute testée par une seule séquence de deux vecteurs d'entrée. La méthode d'estimation de la confiance de test que nous avons développée au chapitre 4 met en évidence le fait que les fautes les plus difficiles à tester déterminent la performance du test. Il faut donc les identifier avec précision. C'est pourquoi nous nous sommes intéressés tout particulièrement au test des transistors collés ouverts.

6 . 4 . 1 . Test par mesure de courant

Le test par mesure de courant est souvent cité pour détecter les courts-circuits et les collages fermés. Nous allons montrer dans ce paragraphe qu'il peut être très efficace pour tester certaines fautes de transistors collés ouverts pour lesquelles le test logique n'est pas toujours possible.

a - Principe

Le test par mesure de courant consiste à mesurer une consommation excessive du circuit du fait de la faute qui l'affecte. Un courant de fuite existe s'il y a un chemin conducteur entre l'alimentation et la masse. Une branche dont le potentiel est compris strictement entre la masse et le potentiel d'alimentation crée un tel chemin conducteur. On appellera **niveau dégradé** un potentiel compris strictement entre la masse (0 V) et la tension d'alimentation (5 V). Un exemple permet de montrer comment un niveau dégradé peut introduire des fuites. Soit l'inverseur CMOS de la figure 6.8a. Le courant statique qui traverse les transistors N et P dépend du potentiel d'entrée V_i. La courbe de la figure 6.8b le montre.

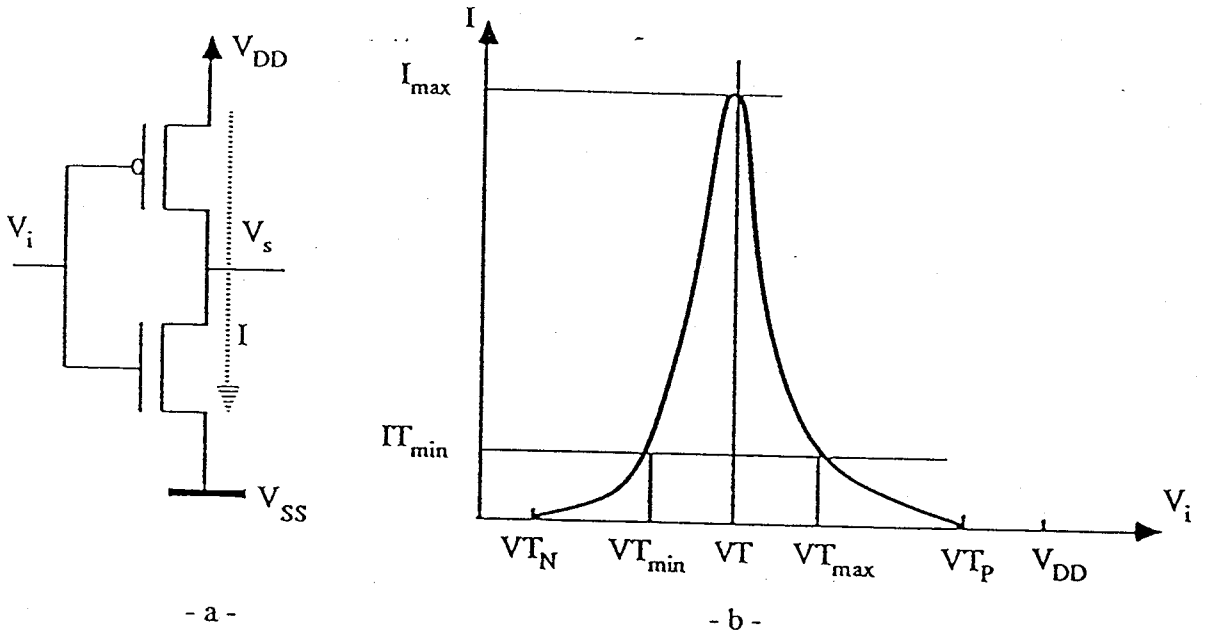


Figure 6.8 : Courant de fuite dû à un niveau dégradé
a - Inverseur CMOS
b - Courant à travers le transistor.

Dans un circuit sans faute le potentiel V_i est égal à 0 ou à V_{DD}. Le courant I est alors nul (quelques **picoampères**). Mais en présence d'une faute le potentiel V_i peut être compris entre les tensions de seuil des transistors N et P, V_{TN} et V_{TP} respectivement. Les transistors N et P sont alors passants. Il apparaît un courant statique non négligeable. Près de V_T le courant atteint un maximum I_{max} de l'ordre de quelques centaines de **microampères**. En d'autres termes si V_i est proche de V_T le courant de fuite est égal à 10^8 fois le courant statique d'un circuit sans faute. Près de V_{TP} ou V_{TN} le courant de fuite est faible. Compte tenu du fait que la consommation statique normale d'un circuit dans son ensemble est de quelques microampères ce courant n'est pas mesurable. Soit IT_{min} le courant de fuite minimum d'une porte défectueuse que l'on peut mesurer (IT_{min} dépend de la consommation de tout le circuit lorsqu'il est sans faute). Soient VT_{min} et VT_{max}

les deux valeurs de V_i qui induisent un courant de fuite égal à IT_{min}. La mesure de courant permet de détecter les fautes qui introduisent un niveau dégradé V_i compris entre VT_{min} et VT_{max}.

Pour une technologie CMOS 2µ dans laquelle $VT_P = 4,4$ V et $VT_N = 0,6$ V pour un inverseur standard et pour $IT_{min} = 10$ µA nous avons trouvé $VT_{min} = 0,9$ V et $VT_{max} = 3,85$ V. Donc toutes les fautes qui créent un potentiel compris entre 0,9 V et 3,85 V sont détectées par une mesure de courant. Dans le cas général d'une porte CMOS complexe les bornes VT_{min} et VT_{max} sont pratiquement inchangées. Par exemple pour une porte Nand à 5 entrées on trouve $VT_{min} = 0,9$ V et $VT_{max} = 3,85$ V si V_i est un niveau dégradé sur une entrée de cette porte. Pour une porte Nor à 5 entrées on trouve $VT_{min} = 0,9$ V et $VT_{max} = 3,75$ V. On peut donc conclure que *toute faute qui crée un potentiel compris entre* **0,95 V** *et* **3,7 V** *en entrée d'une porte CMOS complexe est détectée par une mesure de courant.*

b - Application aux transistors collés ouverts

Lorsqu'un noeud est dans un état de haute impédance sa charge évolue dans le temps du fait des résistances de fuite qui existent dans le circuit. Un niveau dégradé apparaît [Levi 81]. Ce phénomène permet d'envisager un test par mesure de courant des transistors collés ouverts. Pour que le courant de fuite soit mesurable ce test doit être réalisé à basse fréquence.

Ce n'est pas ce phénomène que nous étudions. Nous allons montrer que le test par mesure de courant peut permettre de détecter, à vitesse nominale, certaines fautes de transistor collé ouvert qui ne sont pas détectables par un test logique. Certaines fautes de transistor collé ouvert introduisent des niveaux dégradés dans un circuit CMOS. C'est le cas dans les portes de transfert.

b - 1) Portes de transfert :

Une porte de transfert est décrite à la figure 6.9. Lorsque C = 1 les deux transistors N et P sont passants, la variable E est connectée à la sortie S. Lorsque C = 0 les deux transistors N et P sont bloqués, la sortie S est dans un état de haute impédance et conserve la valeur qu'elle avait précédemment.

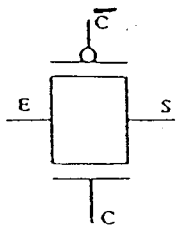


Figure 6.9 : Porte de transfert

Supposons que le transistor P soit collé ouvert (le résultat est dual si le transistor N est

collé ouvert). Le transistor N seul ne peut pas faire passer la sortie de 0 V à 5 V. Cette faute introduit un niveau logique 1 dégradé. Aucune erreur logique n'apparaît mais les performances du circuit sont modifiées. En particulier le niveau 1 dégradé ne permet pas de bloquer les transistors P qu'il commande. En aval de la porte défectueuse les transistors N et P commandés par S sont conducteurs (figure 6.10). Il peut exister un chemin conducteur entre V_{DD} et V_{SS}. Il y a consommation de courant statique et les temps de commutation sont plus grands.

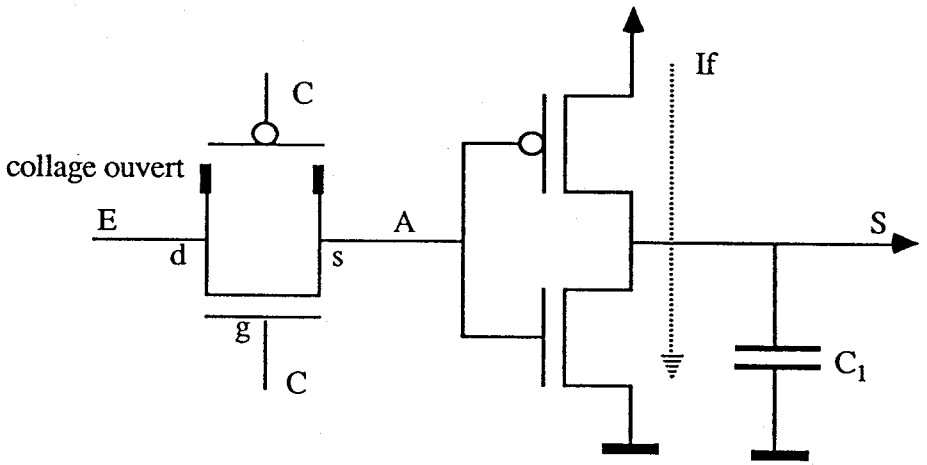


Figure 6.10 : Transistor P collé ouvert dans une porte de transfert

Les équations électriques qui régissent le fonctionnement d'un transistor permettent de majorer le potentiel V_A de sortie de la porte défectueuse [Mead 79]. Pour la technologie CMOS 2µ déjà mentionnée on peut calculer :

$$V_A \geq 3{,}95 \text{ V} = V_{Amax}$$

La valeur V_{Amax} est supérieure au seuil de l'inverseur, la valeur logique en S est donc correcte. Cependant cette faute introduit deux types de mauvais fonctionnements :

1) le courant qui traverse le transistor N de l'inverseur est plus petit que dans un circuit sans faute car le potentiel V_A est trop faible pour rendre ce transistor complètement passant. La capacité C_1 se décharge alors plus lentement ce qui entraine une augmentation DTP du temps de propagation TP à travers la porte.

2) le potentiel V_A ne permet pas de bloquer complètement le transistor P de l'inverseur. Il y a donc un courant statique If qui traverse l'inverseur puisque les deux transitors N et P sont conducteurs.

La simulation de cette faute a conduit aux résultats suivants :

1) si le transistor P est collé ouvert alors V_{Amax} = 3,95 V, TP = 0,85 ns, DTP = 0,5 ns et If = 7 µA .

2) si le transistor N est collé ouvert alors V_{Amin} = 1,1 V, TP = 0,95 ns, DTP = 2,8 ns et If = 35 µA .

Il apparaît clairement que If et DTP sont liés. Une grande augmentation du temps de propagation DTP peut introduire un mauvais fonctionnement mais dans ce cas le courant de fuite peut être détecté facilement par une mesure de courant.

Remarque 6.2 : De manière plus générale on peut envisager de tester les fautes de transistor collé ouvert en testant les fautes de délai du circuit. En effet si une séquence de test détecte toutes les fautes de délai dans un circuit CMOS statique alors cette séquence détecte toutes les fautes de transistor collé ouvert dans le circuit [David 88].

□

b - 2) Collages ouverts et dévalidation :

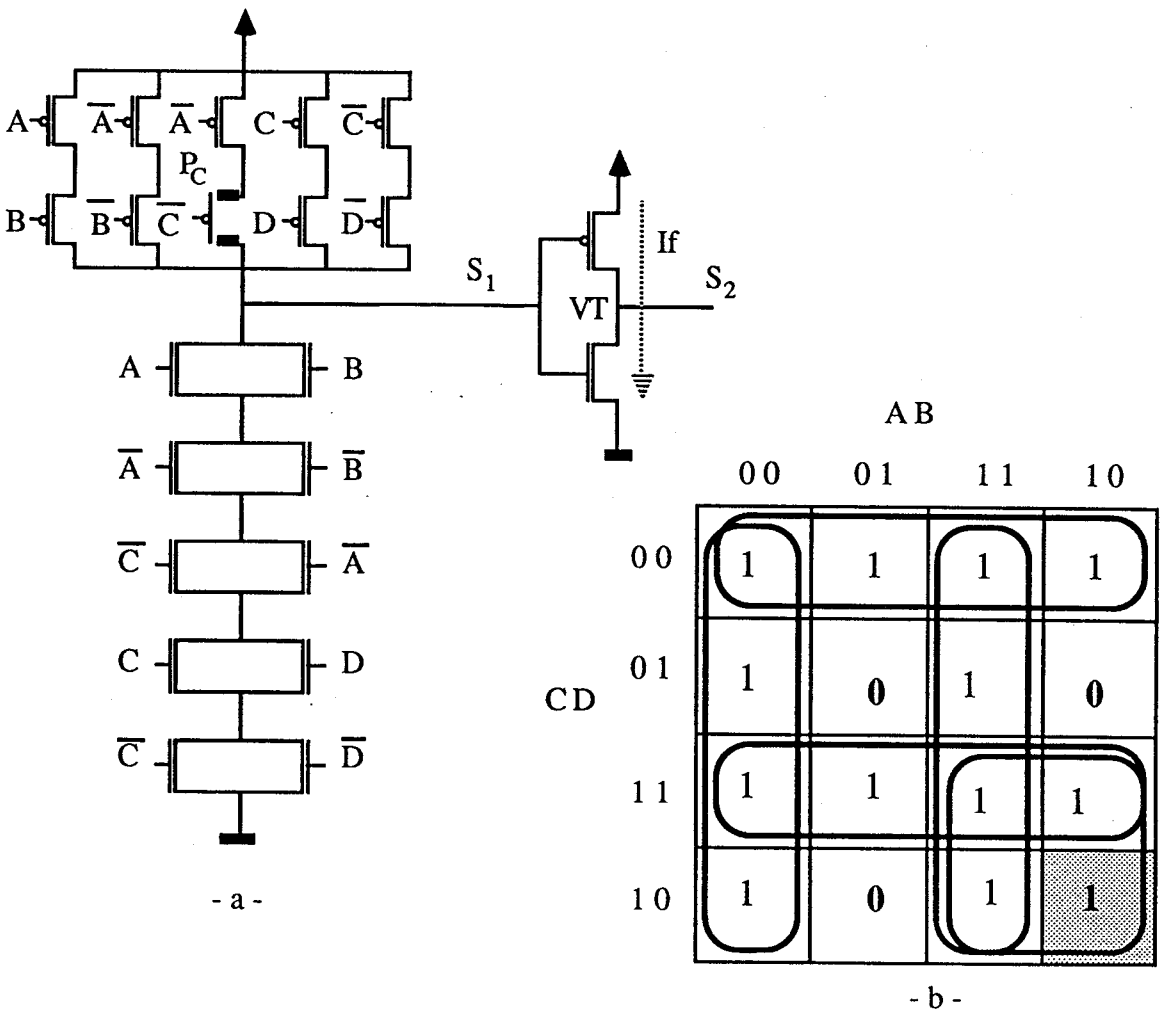


Figure 6.11 : Porte proposée dans [Reddy 83]
a - Description de la porte b - Tableau de Karnaugh

Dans certaines portes complexes il existe des fautes de transistor collé ouvert pour lesquelles il n'existe pas de vecteur de test adjacent à un vecteur d'initialisation. Dans ce cas le test logique de ces fautes peut ne pas être possible à cause des délais de propagation dans le circuit. Ce phénomène a été mis en évidence dans [Reddy 83] à partir de la porte décrite à la figure 6.11.

Cette porte réalise la fonction F = AB + A'B' + AC + CD + C'D'. Soit $T = V_A V_B V_C V_D$ un vecteur tel que V_i est le niveau logique de l'entrée i. Par exemple T = 1011 correspond à A = C = D = 1 et B = 0. Supposons que le transistor P_C, le transistor commandé par C dans le terme AC, soit collé ouvert. Un vecteur d'initialisation T_1 doit mettre la sortie S à 0. On a donc T_1 = 1001 ou 0101 ou 0110. Le vecteur de test T_2 doit mettre la sortie à 1 si le circuit est sans faute et dans un état de haute impédance si P_C est collé ouvert. Le seul vecteur de test possible est T_2 = 1010. Il n'existe pas de vecteur T_1 adjacent au vecteur T_2, chaque séquence T_1T_2 est sensible aux délais de propagation inhérents au circuit. On voit à la figure 6.11b que pour passer d'un vecteur T_1 qui met la sortie S à 0 au vecteur T_2 il faut passer de façon transitoire par un vecteur T_T qui met la sortie S à 1. Si cet état transitoire dure assez longtemps alors l'initialisation du point mémoire à 0 est effacée et le vecteur T_2 ne fait pas apparaître d'erreur en sortie de la porte défectueuse. La figure 6.12 illustre l'influence de la durée de l'état transitoire TD sur le test de la porte défectueuse par la séquence $T_1T_TT_2$ = (1001), (1011), (1010).

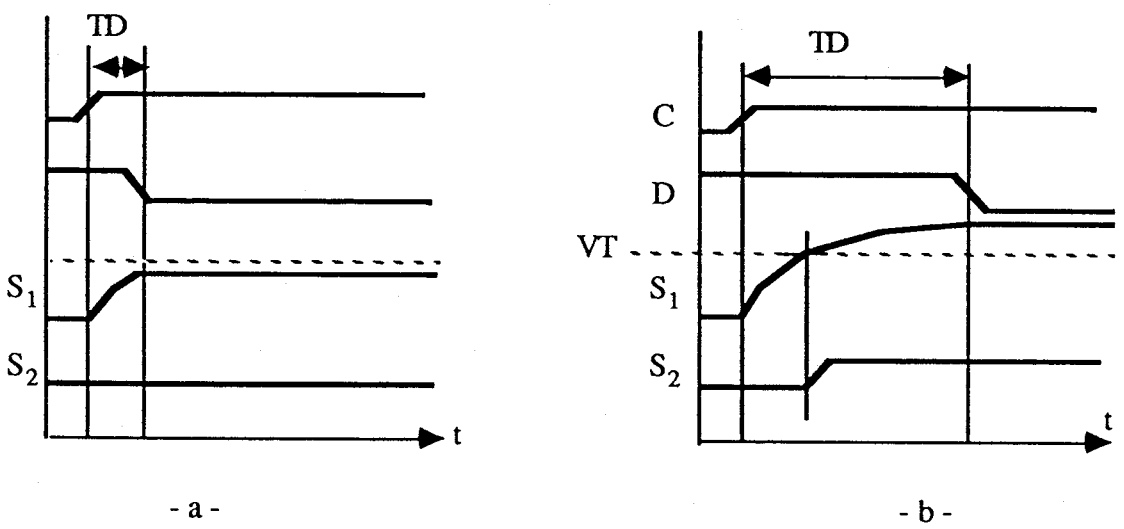


Figure 6.12: Influence de TD pour la porte de Reddy
a -TD petit b - TD grand

Si TD est trop petit (figure 6.12a) pour que la sortie S atteigne la tension seuil V_T de l'inverseur alors le test logique de P_C collé ouvert est possible. Si TD est assez grand pour que S dépasse V_T (figure 6.12b) alors aucune erreur logique n'apparaît en sortie de la porte défectueuse. Toutefois si S atteint une valeur comprise entre VT_{min} et VT_{max} alors un courant de fuite If mesurable traverse l'inverseur. La consommation de courant en fonction de la durée de l'état

transitoire est décrite à la figure 6.13.

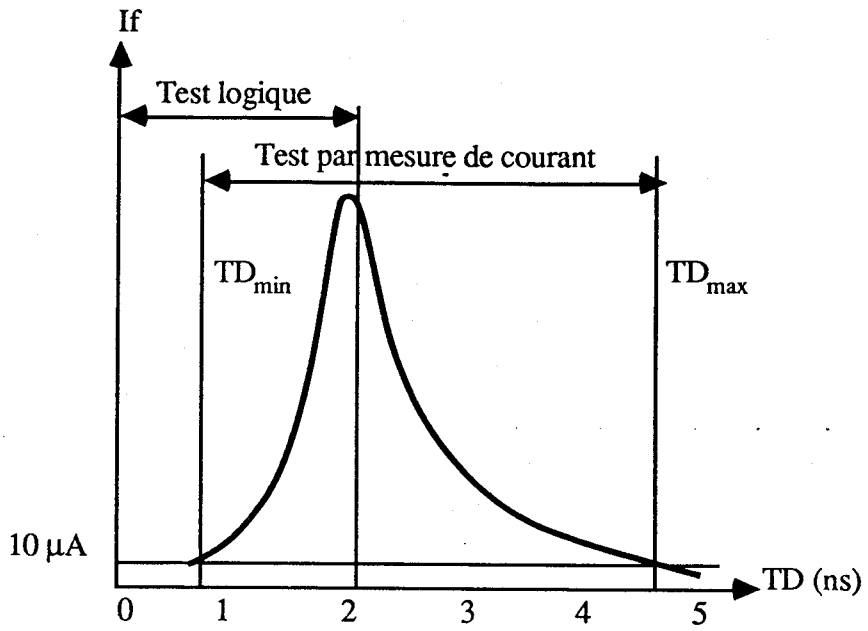


Figure 6. 13 : Influence de TD sur les courants de fuite

On peut voir que pour TD > 2 ns le test logique n'est pas possible ; la mesure de courant permet de détecter P_C collé ouvert pour toute valeur de TD comprise entre **0,7 ns et 4,8 ns**. La mesure de courant permet donc de détecter des fautes de transistor collé ouvert lorsque le test logique n'est plus possible. Dans [Reddy 86] les auteurs présentent des méthodes de conception de circuits CMOS dans lesquels aucune faute de transistor collé ouvert n'est sensible aux délais de propagation dans le circuit.

De façon plus générale, on montre dans [Jacomino 86] que le test par mesure de courant est très efficace pour détecter différents types de fautes dans les circuits CMOS.

Nous avons montré dans cette partie que le test par mesure de courant permet, en particulier, de détecter un transistor collé ouvert dans une porte de transfert. Les portes de transfert sont très utilisées pour réaliser un multiplexeur. Elles sont de ce fait relativement nombreuses dans un circuit tel qu'un microprocesseur. Il ne nous paraît pas réaliste de négliger de les tester, c'est pourquoi nous nous sommes attachés à montrer que ces fautes sont détectables par une séquence de deux vecteurs.

6 . 4 . 2 . Sensibilité d'un transistor à un collage ouvert

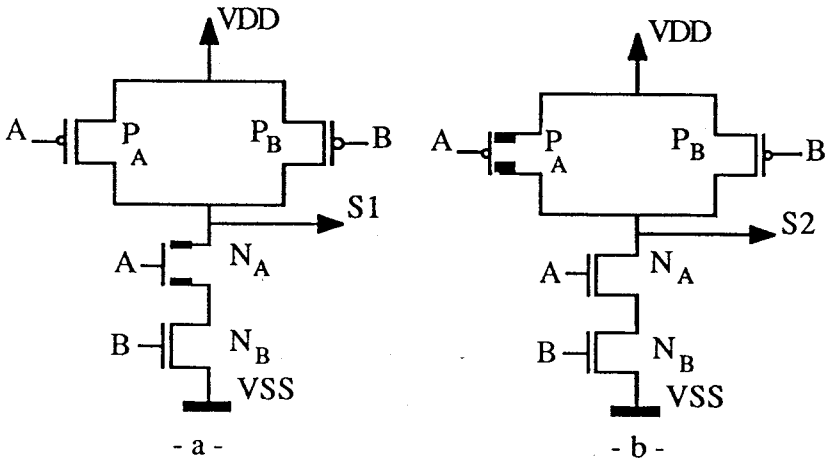
Pour un circuit CMOS nous avons retenu deux classes de fautes possibles : d'une part les fautes testées par au moins un vecteur d'entrée et d'autre part les fautes testées par au moins une séquence de deux vecteurs d'entrée. Dans cette seconde classe nous n'avons retenu que les collages ouverts. Ces fautes sont les plus difficiles à tester. Nous allons montrer que dans un circuit CMOS tous les transistors ne sont pas sensibles à une faute de collage ouvert.

Définition 6.1 : Dans un circuit CMOS un transistor P (resp. N) est **sensible** à une faute de collage ouvert si, lorsqu'il est collé ouvert, il existe au moins un vecteur d'entrée qui connecte la sortie de la porte défectueuse à l'alimentation (resp. la masse).

□

Exemple : Soit la porte Nand de la figure 6.14a dont le transistor N commandé par A est collé ouvert.

La sortie de la porte défectueuse est alors isolée de la masse. En effet aucun vecteur d'entrée ne permet de connecter S_1 à V_{SS} comme le montre le tableau de la figure 6.14c. Après que la sortie ait été mise à 1 elle ne peut plus jamais prendre la valeur 0 du fait de la faute. On peut donc assimiler le collage ouvert d'un transistor N dans une porte Nand au collage à 1 de la sortie. On dit que les transistors N d'une porte Nand ne sont pas sensibles au collage ouvert. Il n'y a que dans l'état initial que S_1 peut être à 0. Si la porte a quitté l'état initial, l'initialisation du point mémoire n'est pas nécessaire pour détecter un transistor N collé ouvert.



A	B	So	S1	S2
0	0	1	1	1
1	0	1	1	1
0	1	1	1	x
1	1	0	x	0

- c -

Figure 6.14 : Transistors sensibles dans une porte NAND

Si le transistor P commandé par A est collé ouvert (figure 6.14b) il existe des vecteurs d'entrée qui connectent S_2 à l'alimentation (figure 6.14c). La valeur mémorisée dans S_2 lorsqu'on applique le vecteur de test T_2 = AB = 01 dépend du vecteur qui a été appliqué avant T_2. La phase

d'initialisation du point mémoire est donc nécessaire pour détecter la faute. Le test d'un transistor P collé ouvert dans une porte Nand est séquentiel (il nécessite une séquence de deux vecteurs d'entrée). On dit que les transistors P d'une porte Nand sont sensibles au collage ouvert.

□

Une faute de transistor collé ouvert qui affecte un transistor qui n'est pas sensible à cette faute n'est pas plus difficile à tester qu'un collage classique. Une telle faute appartient à la classe A définie par Thorel. Nous proposons de dénombrer les transistors sensibles à une faute de collage ouvert dans les portes CMOS suivantes : l'inverseur, la porte Nand, la porte de transfert, la porte OU Exclusif, la bascule maître esclave.

a - La porte Nand

Nous avons vu dans l'exemple précédent que les *transitors N d'une porte Nand ne sont pas sensibles* à un collage ouvert alors que les *transistors P le sont.*

b - L'inverseur

Dans un inverseur CMOS (figure 6.3) il n'existe qu'un seul chemin V_{DD}-S (resp. V_{ss}-S) à travers un transistor P (resp. N). Si ce transistor (P ou N) est collé ouvert la sortie est isolée de l'alimentation (resp. la masse). Les deux transistors N et P d'un inverseur CMOS ne sont donc *pas sensibles à un collage ouvert.*

c - La porte de transfert

Une porte de transfert n'est pas une porte Full-CMOS. Dans son fonctionnement normal lorsque la porte de transfert est passante (C = 1) les deux transistors N et P sont passants, lorsque la porte est fermée (C = 0) les deux transistors sont bloqués (figure 6.9) et la sortie est dans un état de haute impédance sans qu'il y ait de mauvais fonctionnement. Nous avons vu au paragraphe 6.4.1 que lorsque le transistor P (resp. N) est collé ouvert dans une porte de transfert la sortie ne peut être portée à un niveau logique 1 (resp. 0) correct. La séquence de sortie 01 (resp. 10) n'est pas réalisée parfaitement, le niveau 1 (resp.0) n'est pas transmis intégralement et la sortie prend une valeur analogique. Pour observer les mauvais fonctionnements dus à cette faute (consommation statique, temps de propagation plus grand) il faut observer le passage de 0 à1 (resp. de 1 à 0) de la sortie. Donc si la sortie peut être portée à 1 (resp. 0) sans passer par la porte de transfert défectueuse alors le test de cette faute est séquentiel, il nécessite une séquence de test. Les portes de transfert sont le plus souvent utilisées dans des *multiplexeurs* (figure 6.15). Dans ce cas

les deux transistors d'une porte de transfert sont sensibles à un collage ouvert.

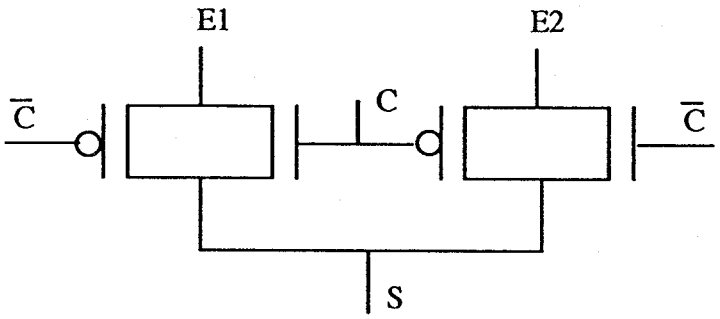


Figure 6.15 : Multiplexage

d - La porte OU Exclusif

La porte OU Exclusif que nous avons choisi d'étudier est représentée à la figure 6.16. La sensibilité aux fautes de collage ouvert de l'inverseur et de la porte de transfert a déjà été étudiée. La sortie S peut être mise à 0 ou à 1 sans passer par la porte de transfert, nous sommes donc dans le cas où cette porte est sensible aux fautes de transistor collé ouvert. Les transistors P_1 et N_1 sont montés en inverseur entre A et $\overline{A}$. Ils n'imposent la valeur de la sortie que lorsque A = 1. Dans ce cas la porte de transfert est bloquée. Lorsque A = 0 la porte de transfert est passante et impose la valeur de la sortie. Donc si un transistor P_1 ou N_1 est collé ouvert la sortie n'est pas collée à 0 ou à 1 du fait de la porte de transfert. Les *transistors P_1 et N_1 sont donc sensibles à une faute de collage ouvert.*

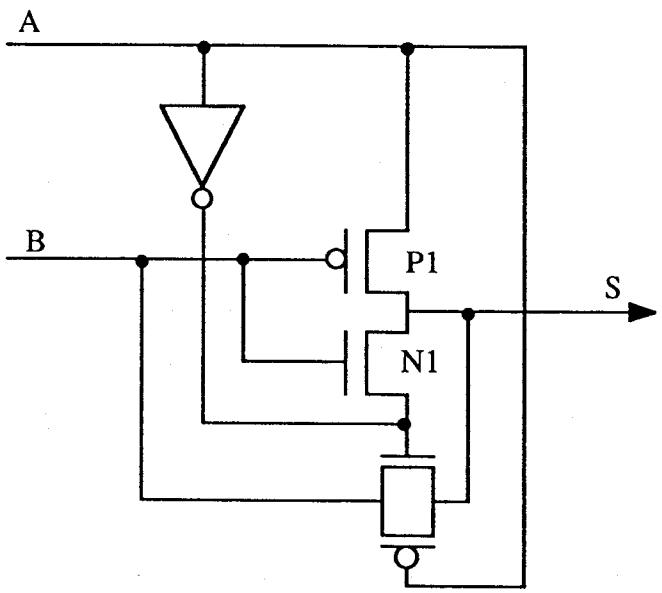


Figure 6.16 : Porte OU exclusif

e - La bascule maître esclave

La bascule maître esclave que nous avons choisi d'étudier est représentée à la figure 6.17.

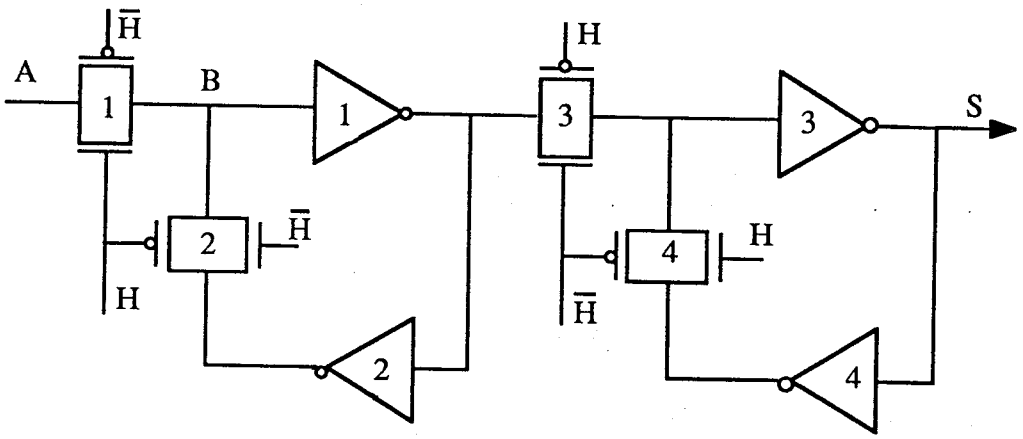


Figure 6.17 : Bascule maître esclave

Lorsque H = 1 la variable d'entrée A est disponible en entrée de l'inverseur 1, elle est mémorisée dans les inverseurs 1 et 2 pendant que la valeur présente au cours de la période précédente est disponible en sortie de la bascule. Lorsque H = 0 la variable mémorisée dans les inverseurs 1 et 2 devient disponible en sortie et est mémorisée dans les inverseurs 3 et 4.

Si un transistor est collé ouvert dans un des deux inverseurs 1 ou 3 la sortie de la bascule est collée à 1 ou à 0. Si le transistor N (resp. P) est collé ouvert dans l'inverseur 2 il y a conflit entre la valeur présente en entrée de l'inverseur 1 et la valeur présente en sortie de l'inverseur 2 si la valeur mémorisée est A = 0 (resp. A = 1). Le point B atteint alors un potentiel d'équilibre qui dépend des couplages capacitifs dans le circuit. La sortie de l'inverseur 2 ne peut prendre que 2 valeurs, soit le niveau logique 1 (resp. 0) soit un niveau dégradé. Dans aucun cas on ne peut avoir 0. Le test du transitor N (resp. P) collé ouvert ne nécessite donc pas d'initialisation. On peut alors conclure qu'*aucun transistor appartenant à un inverseur dans une bascule maître esclave n'est sensible à un collage ouvert.*

Dans la bascule maître esclave les 4 portes de transfert sont utilisées en multiplexeur. Toutefois ces multiplexeurs sont très particuliers. En effet si le transistor N (resp. P) est collé ouvert dans la porte de transfert 1 alors la variable mémorisée dans la bascule ne peut prendre que deux valeurs, soit le niveau logique 0 (resp. 1) soit un niveau dégradé. Dans aucun cas on ne peut avoir 1 (resp. 0) dans la bascule. Le test du transistor N (resp. P) collé ouvert dans la porte de transfert 1 ne nécessite donc pas d'initialisation. De même si le transistor N (resp. P) de la porte de

transfert 3 est collé ouvert on ne peut pas avoir le niveau logique 1 (resp. 0) en sortie de la bascule. Dans les boucles de mémorisation la sortie des portes de transfert (portes de transfert 2 et 4) est en "conflit" avec la même valeur présente dans la branche d'entrée. Si le transistor N (resp. P) est collé ouvert dans la porte de transfert 2 et que la valeur mémorisée est A = 0 il y a conflit en B entre un niveau logique 0 et un niveau 0 dégradé. Le potentiel d'équilibre alors obtenu entraine un courant de fuite mesurable seulement si le circuit est testé à très basse fréquence. Cette faute n'entraine pas de mauvais fonctionnement à vitesse nominale, elle ne rentre donc pas dans les hypothèses de faute retenues. On peut donc conclure qu'*aucun des transistors appartenant à une porte de transfert dans une bascule maître esclave n'est sensible à un collage ouvert.*

Parmi les 16 transistors qui composent une bascule maître esclave, *aucun n'est sensible à une faute de collage ouvert* .

6 . 4 . 3 . Occurrence d'un collage ouvert

L'étude du test d'un transistor collé ouvert que nous avons développée dans cette partie permet de définir l'ensemble F_2 des fautes les plus difficiles à tester dans un circuit CMOS de la façon suivante :

$$F_2 = \{\text{transistors sensibles collés ouverts}\}$$

La probabilité d'occurrence de F_2 s'écrit :

$$Pr [F_2/F] = Pr [\text{un transistor sensible est collé ouvert / F}]$$

La sensibilté d'un transistor à un collage ouvert dépend uniquement de la structure de la porte qui le contient. On a donc :

$$Pr [F_2/F] = Pr [\text{transistor sensible}] \; Pr [\text{transistor collé ouvert / F}]$$

Le terme Pr [transistor sensible] dépend du circuit testé. Nous nous proposons d'estimer la probabilité Pr [transistor collé ouvert / F].

La probabilité d'occurrence d'une faute dans un circuit est un sujet sur lequel peu de résultats sont publiés. Je vois trois raisons à cela : ces chiffres sont propres à chaque fabricant et évoluent aussi vite que la technologie, mais surtout ils ont un caractère confidentiel. Dans [Banerjee 82] les auteurs distinguent 9 types de fautes physiques réparties en 3 classes : les fautes très probables, les fautes moins probables et les fautes les moins probables. Mais la fréquence d'apparition de ces types de défauts n'est pas chiffrée. Baschiera a publié les résultats de tests de vieillissement qui ont permis de mesurer la probabilité d'occurrence de certains mécanismes de

Chapitre 7

Application au microprocesseur MTI

Dans ce chapitre les résultats décrits dans les chapitres pécédents sont mis en oeuvre afin d'estimer de façon précise la longueur de test aléatoire à appliquer à un circuit particulier : le MTI , microprocesseur à test intégré conçu et réalisé au CNET. Les fautes les plus difficiles à tester qui peuvent affecter ce circuit sont identifieés de façon précise et leur probabilité d'occurrence est estimée. La perte de confiance due à l'analyse de signature est abordée dans un second temps.

7 . 1 . Introduction

Le microprocesseur MTI a été réalisé au CNET/CNS de Grenoble. C'est un microprocesseur à test intégré. Le dispositif de test s'appuie sur un générateur de vecteurs pseudo-aléatoire de test et un registre à décalage à rebouclage linéaire comme analyseur de signature. Ce circuit a été conçu en particulier pour valider certaines techniques d'intégration du test. Bien qu'expérimental ce microprocesseur est représentatif de la complexité des circuits que l'on rencontre sur le commerce (30 000 transistors). Nous proposons d'estimer la confiance dans le test du circuit MTI. Après une description du circuit nous appliquerons la méthode d'estimation de la confiance dans la séquence de test développée au chapitre 4 de ce mémoire. Nous étudierons ensuite l'influence de l'analyse de signature sur la performance du test.

7 . 2 . Description du circuit

Le circuit MTI comprend, sur une même puce, un microprocesseur et un dispositif de test. Le microprocesseur a été conçu à partir de spécifications fonctionnelles (les interruptions vectorisées, les registres banalisés, l'adressage étendu), indépendantes de l'intégration du test. Il a été conçu pour être facilement testable par un test aléatoire. Le dispositif de test a été rajouté à ce "circuit nominal" [Thorel 87b].

7 . 2 . 1 . Microprocesseur

Le microprocesseur exécute un programme implanté sur une mémoire externe qui contient également les données du programme. L'architecture du MTI est organisée autour d'un **bus unique** de 16 bits. Une mémoire interne RAM de 64 mots de 16 bits réalise les 32 registres banalisés, les 12 doubles mots d'état programme et les 8 bases d'adressage. L'Unité Arithmétique et Logique (UAL) effectue des opérations sur 16 bits portant sur deux opérandes. Le séquenceur,

organisé autour d'un PLA unique, interprète les 64 instructions possibles. Il existe 12 niveaux d'interruption dont 7 sont activables de l'extérieur.

7 . 2 . 2 . Dispositif de test

Le test du circuit MTI est appliqué *à travers le bus* : en **mode test** les vecteurs aléatoires de test sont injectés sur le bus se substituant à la mémoire externe. Un registre à décalage à rebouclage linéaire comportant 31 bascules génère les vecteurs aléatoires. Seulement 21 bits sont utilisés : 16 bits sont connectés au bus, 3 bits constituent un vecteur d'interruption aléatoire et 2 bits équiprobables sont nécessaires pour améliorer la testabilité de certaines parties du circuit. Les données générées connectées au bus traversent les plots d'Entrée/Sortie. Le générateur aléatoire est tel que les vecteurs générés aux instants t et t+1 sont indépendants. Un dispositif d'observation des résultats est également implanté dans le circuit MTI. Il est constitué d'un registre à décalage à rebouclage linéaire de 61 bascules. Les données compactées sont les sorties du circuit nominal et certaines données internes ; soit au total 61 données. Lorsque la séquence de test a été entièrement appliquée un plot permet la sortie en série de la signature. La longueur de test aléatoire d'un circuit croît avec la complexité du circuit. Pour être "facilement" testable un circuit ne doit pas dépasser une certaine complexité. Pour le MTI la durée maximale de test admise (1 s à 20 MHz) a déterminé la longueur de test à ne pas dépasser (L = 20 000 000 cycles). Afin que 20 000 000 cycles permettent de tester le circuit tout en assurant le niveau de confiance exigé il a été nécessaire de partitionner le circuit. Le **partitionnement** consiste à diviser le circuit en sous-circuits plus petits. Dans le MTI cette décomposition a été réalisée en insérant des données aléatoires entre les sous-circuits et en observant les sorties de ces sous-circuits.

Un dispositif de test par **mesure de courant** a également été implanté dans le circuit. Il comprend essentiellement des amplificateurs opérationnels.

Au total la surface de silicium occupée par le dispositif de test a été estimée à **14%** de la **surface totale.**

7 . 3 . Confiance dans le test du circuit MTI

Nous proposons dans cette partie d'estimer la confiance dans la méthode de test appliquée au MTI. Le niveau de confiance exigé est tel que au plus un circuit défectueux sur 1 000 passe la test. C'est-à-dire $*P_a \geq 0{,}999$. Compte tenu de la confiance que l'on veut obtenir il faut calculer la longueur de la séquence de test à appliquer. Il s'agit de traiter le problème dual de celui développé jusque là : quelles sont les caractéristiques (ici la longueur de test) qui permettent de

remplir les exigences de confiance fixées *a priori* ? Pour résoudre ce problème nous allons utiliser le théorème 5.5 ($^*P_a \geq P_a P_{Am}$) et étudier d'une part la confiance dans la séquence de test et d'autre part la confiance dans l'analyseur de signature.

7 . 3 . 1 . Confiance dans la séquence de test

Dans cette partie nous allons appliquer au circuit MTI le principe de partition de l'ensemble de fautes prescrit pour estimer la longueur de test qui assure $\mathbf{P_a \geq 0{,}999}$. On suppose que les fautes qui peuvent affecter le circuit appartiennent soit à la classe A soit à la classe B. C'est-à-dire que toutes les fautes prescrites sont testées par au moins une séquence de deux vecteurs d'entrée.

Soit $\mathbf{L_{MTI}}$ la longueur de test appliquée au circuit MTI. Pour estimer cette longueur le circuit peut être décomposé en quatre parties : le *séquenceur* noté CS, la *mémoire interne* RAM notée RAM, le *chemin de données* noté DP et le *dispositif de test* noté T. Lorsque le dispositif de test est externe au circuit le résultat du test "bon/mauvais" doit porter sur l'état du circuit. Il faut éviter que le mauvais fonctionnement du dispositif de test entraine la destruction de circuits sans faute. Lorsque la dispositif de test est intégré au circuit et qu'aucun diagnostic n'est envisagé, on peut considérer que le dispositif de test est un composant du circuit. Ceci est encore plus vrai lorsque les éléments qui composent le dispositif de test ont également un rôle fonctionnel. C'est le cas dans le circuit MTI où le registre de signature est constitué de bascules qui ont une fonction en mode normal. Il faut s'assurer dans ce cas que le dispositif de test est lui même testé. Le résultat du test *"bon/mauvais"* porte alors sur l'*ensemble de la puce* qui est globalement utilisée ou rejetée. Cette partition du circuit en quatre sous-circuits correspond à une décomposition de l'ensemble de fautes prescrit, $F = \{F_{CS}, F_{RAM}, F_{DP}, F_T\}$ dans laquelle F_X représente l'ensemble des fautes qui peuvent affecter la partie X. Pour chacun de ces sous-circuits une étude de pire cas a été développée par Thorel dans [Thorel 87a] qui a conduit aux résultats suivants :

Pour la faute la plus difficile à tester dans le séquenceur,

$$L_{CS} = 400\,000 \text{ cycles, pour } P_m(F_{CS}) = 0{,}999$$

Pour la faute la plus difficile à tester dans la mémoire RAM,

$$L_{RAM} = 800\,000 \text{ cycles, pour } P_m(F_{RAM}) = 0{,}999$$

Pour la faute la plus difficile à tester dans le chemin de données,

$$L_{DP} = 16\,000\,000 \text{ cycles, pour } P_m(F_{DP}) = 0{,}999$$

Pour la faute la plus difficile à tester dans le dispositif de test ,

$$L_T << 400\,000 \text{ cycles, pour } P_m(F_T) = 0{,}999.$$

(7.1)

Dans le MTI le dispositif de test comprend des éléments qui sont très faciles à tester. Le générateur de vecteurs de test applique ses sorties sur le bus qui est directement observable. Le registre de signature est constitué de bascules qui ont une fonction dans le circuit nominal donc une faute dans ce registre est une faute du circuit, cette faute est directement observable. Les portes OU exclusif ajoutées en plusieurs endroits du circuit sont facilement commandables (une de leurs entrées provient du générateur de vecteurs de test) et observables (leurs sortie est presque toujours connectée au registre de signature). Tous les éléments qui composent le dispositif de test sont au moins aussi faciles à tester que toutes les autres parties du circuit nominal.

La longueur de test qui a été retenue lors de l' étude de Thorel est

$$L_{MTI} = \max (L_{CS}, L_{RAM}, L_{DP}, L_T)$$

soit

$$\mathbf{L_{MTI} = L_{DP} = 16\ 000\ 000 \text{ cycles}}$$

Cette longueur assure $\mathbf{P_m \geq 0{,}999}$.

La confiance de test obtenue dépasse la confiance de test exigée puisque $P_a \geq P_m$. Nous allons montrer que la longueur de test qui assure $P_a = 0{,}999$ peut être approchée en étudiant différentes partitions de l'ensemble de fautes prescrit.

a - Principe de la méthode

A l'aide de partitions de plus en plus efficaces de l'ensemble de fautes prescrit, la probabilité minimum pondérée de test permet d'estimer de plus en plus précisément la confiance dans la séquence de test. A partir d'une décomposition assez grossière du MTI nous allons étudier de plus en plus précisément les fautes les plus difficiles à tester. Nous verrons qu'il n'est pas nécessaire d'étudier les fautes faciles à tester.

Dans un premier temps nous considèrerons les *4 classes* de fautes relatives aux 4 sous-circuits du MTI : les fautes qui affectent le séquenceur, les fautes qui affectent la RAM, les fautes qui affectent le chemin de données et les fautes qui affectent le dispositif de test ($\rho = \{F_{CS}, F_{RAM}, F_{DP}, F_T\}$). La figure 7.1 représente la décomposition en 4 blocs de l'ensemble de fautes prescrit. Les résultats obtenus par Thorel montrent que la faute la plus difficile à tester affecte le chemin de données. Les autres parties du circuit sont beaucoup plus faciles à tester que le chemin de données. On verra que leur probabilité minimum de test par un vecteur est égale à plus de 20 fois la probabilité minimum de test par un vecteur du chemin de données. On considérera la partition suivante : $\rho = \{F_1, F_2\}$ avec F_2 les fautes qui affectent le chemin de données et F_1 toutes les autres fautes.

La suite de notre étude consistera à distinguer parmi les fautes qui affectent le chemin de données celles qui sont *réellement difficiles à tester* et en particulier celles qui sont plus difficiles à tester que la RAM. En d'autres termes nous allons faire passer des fautes de l'ensemble F_2 (des fautes éventuellement difficiles à tester) vers l'ensemble F_1 des fautes faciles à tester. La figure 7.2 illustre les différentes étapes qui permettent de différencier les fautes les plus difficiles à tester.

Thorel dans [Thorel 87a] désigne la faute la plus difficile à tester dans le chemin de données comme étant un *transistor collé ouvert dans l'Unité Arithmétique et Logique* (UAL). Par ailleurs on montre que les autres fautes qui peuvent affecter le chemin de données sont au moins aussi faciles à tester que la mémoire RAM. Les fautes les plus difficiles à tester et qui appartiennent à F_2 sont donc les fautes de transistor collé ouvert dans l'UAL. Cette caractérisation de la faute la plus difficile à tester permet d'une part de la **localiser** avec précision (dans l'UAL) et d'autre part de différencier les fautes à travers le mauvais fonctionnement qu'elles entrainent (**nature des fautes**)(figures 7.2a et 7.2b) : pour un même transistor on distingue les collages ouverts des autres fautes qui peuvent l'affecter (collage fermé, collage classique).

Nous ferons ensuite une étude précise des fautes de transistor collé ouvert dans l'UAL. A partir de l'étude détaillée des transistors sensibles à un collage ouvert développée dans le paragraphe 6.4.2 nous dénombrerons les transistors sensibles dans l'UAL. Le collage ouvert d'un transistor qui n'est pas sensible n'est pas une faute parmi les plus difficiles à tester. On pourra alors restreindre F_2 aux seules fautes réellement difficiles à tester, c'est-à-dire aux fautes de collage ouvert des *transistors sensibles* de l'UAL (figure 7.2c).

Enfin, nous montrerons que l'hypothèse pessimiste qui consiste à dire qu'un transistor collé ouvert est testé par *une seule* séquence de deux vecteurs d'entrée, n'est pas vérifiée pour les transistors difficiles à tester dans le MTI. Compte tenu du nombre réduit de transistors à étudier (46) nous avons calculé les probabilités de test et d'occurrence de toutes les fautes les plus difficiles à tester. La figure 7.3 illustre la répartition des fautes difficiles à tester. Ceci nous a permis de calculer **2 bornes de P_a** très proches l'une de l'autre (figure 7.2d).

Nous allons voir maintenant numériquement comment cette démarche permet d'estimer **P_a à 10^{-5} près** (compte tenu des hypothèses sur les probabilités d'occurrence des fautes que nous allons présenter, et sous réserve des erreurs d'arrondi que nous faisons de façon à manipuler des nombres plus "lisibles").

b - Application numérique

A partir de l'étude de pire cas qui a été développée par Thorel nous pouvons étudier la

partition $\rho = \{F_{CS}, F_{RAM}, F_{DP}, F_T\}$. Pour calculer $P_w(\rho)$ il faut connaître la probabilité d'occurrence de chaque bloc et la probabilité minimum de test de chaque bloc.

b . 1) Probabilités d'occurrence :

Hypothèse 7.1 : La probabilité qu'a chaque sous-circuit d'être défectueux est proportionnelle au nombre de transistors qui le composent.

□

Cette hypothèse peut se justifier dans un circuit CMOS où tous les modèles de faute peuvent être rapportés au transistor.

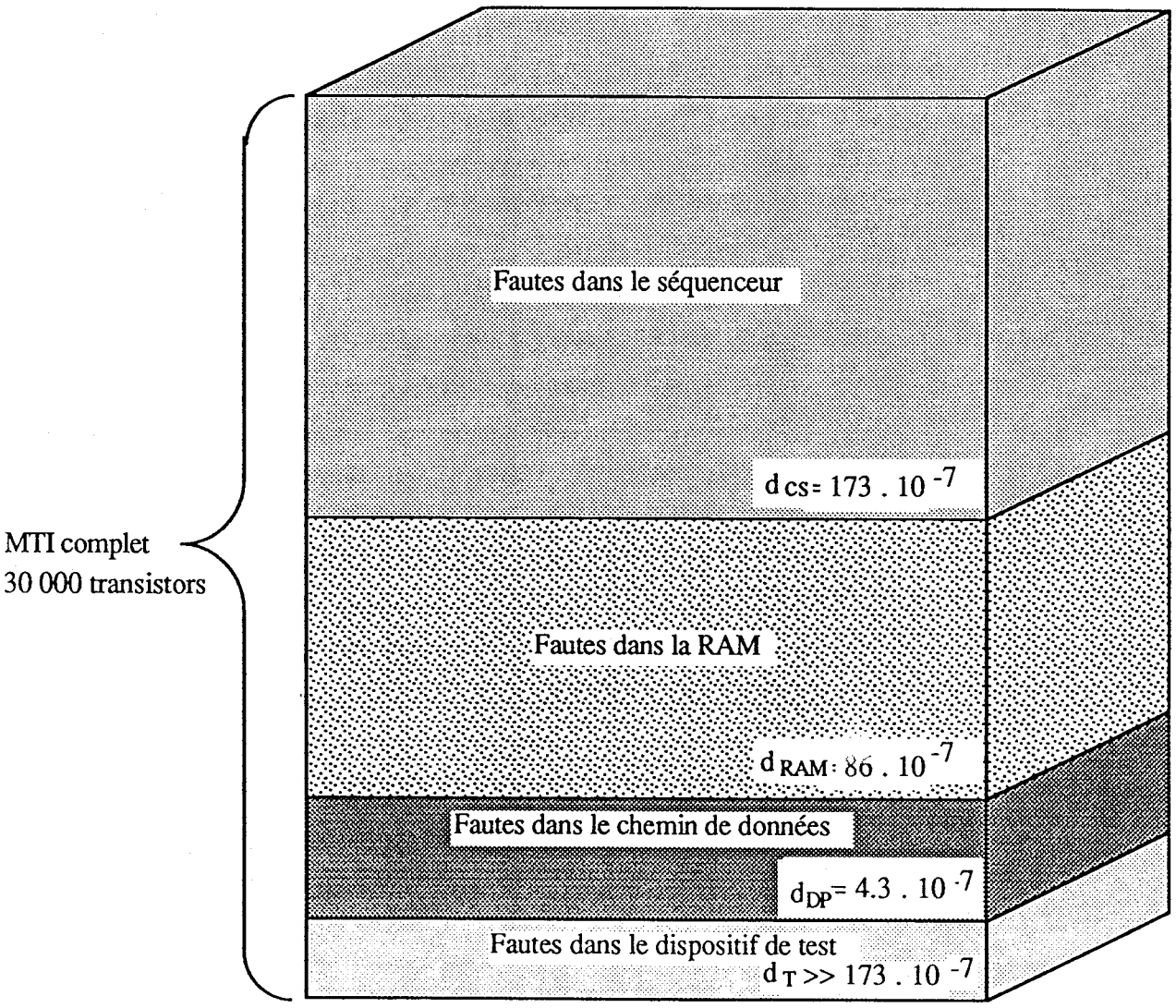


Figure 7.1 : Répartition des fautes dans le MTI

Dans le circuit MTI le séquenceur contient 14 000 transistors, la mémoire RAM contient

9 000 transistors, le chemin de données contient 4 500 transistors et le dispositif de test contient 2 500 transistors. On peut donc calculer :

$$Pr\,[F_{CS}/F] = \frac{14\,000}{30\,000} = 0{,}467$$

$$Pr\,[F_{RAM}/F] = \frac{9\,000}{30\,000} = 0{,}3$$

$$Pr\,[F_{DP}/F] = \frac{4\,500}{30\,000} = 0{,}15$$

$$Pr\,[F_{T}/F] = \frac{2\,500}{30\,000} = 0{,}083$$

La figure 7.1 représente la proportion de transistors contenue dans chaque sous-circuit.

b.2) Probabilités minimum de test :

Soit d la probabilité de test par un vecteur d'une faute f. Pour une grande longueur de test on peut écrire :

$$P_T(f_i) = 1 - (1- d)^L$$

Les résultats obtenus par Thorel nous permettent d'écrire la relation suivante pour la faute la plus difficile à tester dans chaque bloc de ρ :

$$0{,}999 = 1 - (1 - d_x)^{Lx} \qquad (7.2)$$

L_X et d_X sont respectivement la longueur de test et la probabilité de test par un vecteur de la faute la plus difficile à tester pour chaque partie X du circuit.

A partir des équations (7.1) et (7.2) on peut calculer :

$$\mathbf{d_{CS} = 173 .10^{-7}}$$

$$\mathbf{d_{RAM} = 86 . 10^{-7}}$$

$$\mathbf{d_{DP} = 4{,}3 .10^{-7}}$$

$$\mathbf{d_{T} >> 173.10^{-7}}$$

La précision de ces résultats dépend des longueurs de test calculées pour chaque sous-circuit. A partir des probabilités minimum de test et d'occurrence de chaque bloc on peut calculer :

$$P_w(\rho) \geq 0{,}467\,(1 - (1 - 173 . 10^{-7})^L) + 0{,}3\,(1 - (1 - 86 . 10^{-7})^L) + 0{,}15\,(1 - (1 - 4{,}3 . 10^{-7})^L) + 0{,}083\,(1 - (1 - 173 . 10^{-7})^L) \qquad (7.3)$$

Pour $P_w(\rho) = 0{,}999$ on trouve **L = 11 660 000 cycles** (il s'agit d'un nombre arrondi).

A partir de l'analyse du circuit qui a été nécessaire pour calculer L_{MTI} telle que $P_m = 0{,}999$ on a pu réduire de près d'**un tiers** la longueur de test simplement en écrivant l'exigence de test de manière plus appropriée.

Remarque 7.1 : Les fautes difficiles à tester sont celles qui déterminent la longueur de test. En effet pour L = 11 660 000 cycles on a $P_m(F_{CS}) \approx P_m(F_{RAM}) \approx P_m(F_T) \approx 1$. Si on fait l'approximation que ces probabilités valent 1, on a l'équation :

$$0{,}85 + 0{,}15\,(1 - (1 - 4{,}3 \cdot 10^{-7})^L) = 0{,}999 \qquad (7.4)$$

Cette équation conduit à **L = 11 660 000 cycles.**

En fait le calcul exact donnerait 11 652 637,70 qui est à comparer au résultat exact de l'équation (7.3) qui donne 11 652 637,71. Il est évident que tous ces chiffres ne sont pas réellement significatifs. Ils ont pour seul but de montrer que l'approximation qui consiste à prendre $P_m(F_{CS}) = P_m(F_{RAM}) = P_m(F_T) = 1$, n'introduit pas d'erreur avant le dixième chiffre.

□

On vérifie dans ce cas que la probabilité de test des fautes qui ne sont pas difficiles à tester n'intervient pas dans le calcul de la longueur de test. En particulier on peut obtenir une bonne estimation de L en ne considérant plus que deux blocs : F_1 l'ensemble des fautes au moins aussi faciles à tester que la RAM, F_2 l'ensemble des fautes plus difficiles à tester que la RAM. On a alors :

$$P_w(\rho) = Pr[F_1/F]\,(1 - (1 - 86 \cdot 10^{-7})^L) + Pr[F_2/F]\,(1 - (1 - 4{,}3 \cdot 10^{-7})^L)$$

Une analyse des fautes réellement difficiles à tester nous permettra de calculer plus précisément $Pr[F_2/F]$. Après avoir partitionné l'ensemble de fautes par rapport à la structure du circuit nous allons distinguer les différents types de fautes qui peuvent affecter un circuit CMOS (figure 7.2).

c - Localisation

La faute la plus difficile à tester est un transistor collé ouvert dans l'UAL. Les autres fautes qui affectent le chemin de données sont au moins aussi faciles à tester que la RAM. On peut donc définir l'ensemble des fautes difficiles à tester de la façon suivante (figures 7.2a et 7.2b):

F_2 = {fautes de transistor collé ouvert dans l'UAL}

Les fautes de F_2 sont exclusives, on peut donc écrire :

$$Pr [F_2/F] = Pr [\text{transistor collé ouvert dans l'UAL/F}]$$

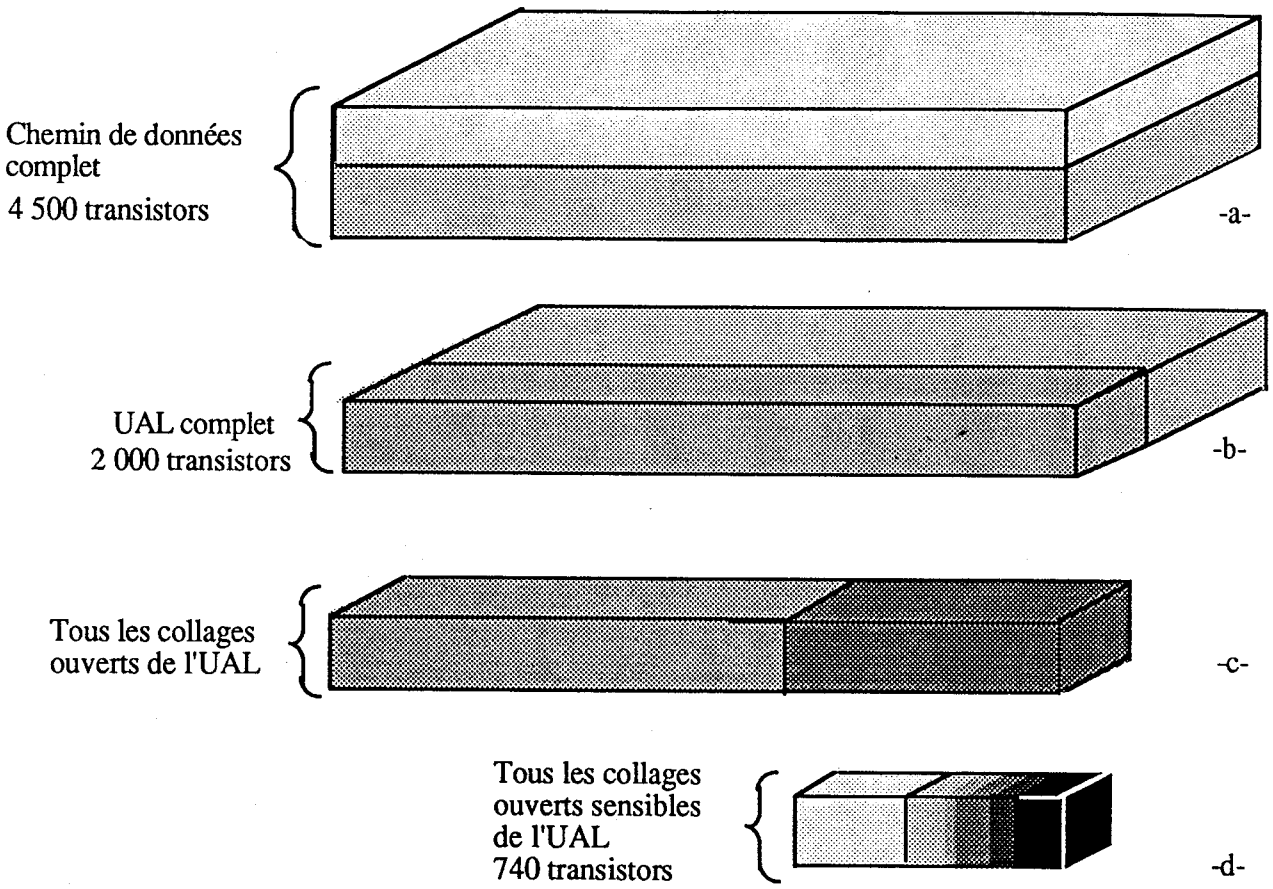


Figure 7.2 : Partition des fautes
a - b - Localisation des fautes les plus difficiles à tester
c - d - Nature des fautes les plus difficiles à tester

L'hypothèse 7.1 implique que tous les transistors ont la même probabilité d'être défectueux, quelle que soit la partie du circuit à laquelle ils appartiennent. L'événement transistor collé ouvert dans l'UAL peut donc être décomposé en deux événements indépendants : transistor collé ouvert et UAL défectueux. On peut alors écrire :

$$Pr [F_2/F] = Pr [\text{UAL défectueux/F}]\ Pr [\text{transistor collé ouvert / F}]$$

L'UAL comprend 2 000 transistors. On a donc d'après l'hypothèse 7.1 :

$$Pr [\text{UAL défectueux/F}] = 0{,}0667$$

Au paragraphe 6.4.3 nous avons calculé :

$$Pr\ [\text{transistor collé ouvert} / F] = 0{,}3636$$

D'où on peut calculer :

$$Pr\ [F_2/F] = 0{,}0667 \times 0{,}3636 = 0{,}02425$$

On a alors :

$$P_w(\rho) = 0{,}97575\ (1 - (1 - 86 \cdot 10^{-7})^L) + 0{,}02425\ (1 - (1 - 4{,}3 \cdot 10^{-7})^L)$$

Pour $P_w(\rho) = 0{,}999$ on trouve **L = 7 420 000 cycles.**

d - Sensibilité

Certaines fautes de transistor collé ouvert sont équivalentes au collage à 1 ou à 0 d'une branche du circuit. Ces fautes sont au moins aussi faciles à tester que la RAM. On peut donc restreindre F_2 aux seules fautes réellement difficiles à tester, c'est-à-dire aux fautes de collage ouvert des transistors sensibles de l'UAL (figure 7.2c) :

$$F_2 = \{\text{fautes de transistor sensible collé ouvert dans L'UAL}\}$$

$$Pr\ [F_2/F] = Pr\ [\text{UAL défectueux}/F]\ Pr\ [\text{transistor sensible collé ouvert} / F]$$

Une tranche de l'UAL est composée de 7 portes Nand, 5 inverseurs, 14 portes de transfert, 1 porte OU exclusif et 3 bascules maître esclave. A partir du nombre de transistors sensibles à un collage ouvert dans chacune de ces portes calculé au paragraphe 6.4.2, on peut dénombrer 46 transistors sensibles parmi les 120 qui composent une tranche de l'UAL. On peut donc calculer :

$$Pr\ [F_2/F] = 0{,}0667 \times 0{,}3636 \times \frac{46}{120} = 0{,}009296$$

$$P_w(\rho) = 0{,}990703\ (1 - (1 - 86 \cdot 10^{-7})^L) + 0{,}009296\ (1 - (1 - 4{,}3 \cdot 10^{-7})^L)$$

Pour $P_w(\rho) = 0{,}999$ on trouve **L = 5 186 000 cycles.**

e - Nombre de séquences de test

La probabilité de test de la faute la plus difficile à tester détermine la longueur de test à appliquer. La probabilité de test par un vecteur égale à $43 \cdot 10^{-7}$ est obtenue pour un transistor collé

ouvert testé par *une seule séquence de deux vecteurs*. En fait nous avons relevé qu'*aucun* des 46 transistors d'une tranche de l'UAL sensible à une faute de collage ouvert n'est testé par une seule séquence de deux vecteurs. Pour chaque transistor sensible de l'UAL nous avons dénombré les séquences de deux vecteurs qui permettent de détecter le collage ouvert. Les résultats sont les suivants :

aucun transistor de l'UAL n'est testé par **une seule** séquence de deux vecteurs d'entrée;
8 transistors de l'UAL sont testés par **2** séquences de deux vecteurs d'entrée ;
6 transistors de l'UAL sont testés par **4** séquences de deux vecteurs d'entrée ;
9 transistors de l'UAL sont testés par **8** séquences de deux vecteurs d'entrée ;
1 transistor de l'UAL est testé par **12** séquences de deux vecteurs d'entrée ;
8 transistors de l'UAL sont testés par plus de **16** séquences de deux vecteurs d'entrée ;
14 transistors de l'UAL sont testés par plus de **48** séquences de deux vecteurs d'entrée . (7.5)

Soient f une faute de transistor collé ouvert dans l'UAL testée par k séquences de deux vecteurs d'entrée, et d sa probabilité de test par un vecteur. On a alors :

$$d = k \times 4{,}3 \cdot 10^{-7}$$

La faute la plus difficile à tester est testée par 2 séquences de deux vecteurs d'entrée ; elle a donc une probabilité de test par un vecteur égale à $8{,}6 \cdot 10^{-7}$ et

$$\mathbf{P_m (F_2) = 1 - (1 - 8{,}6 \cdot 10^{-7})^L}$$

en considérant le même ensemble de fautes difficiles à tester que précédemment. On peut calculer :

$$P_w (\rho) = 0{,}990703 \, (1 - (1 - 86 \cdot 10^{-7})^L) + 0{,}009296 \, (1 - (1 - 8{,}6 \cdot 10^{-7})^L)$$

Pour $P_w (\rho) = 0{,}999$ on trouve **L = 2 600 000 cycles.**

Remarque 7.2 : On voit que la probabilité de test de la faute la plus difficile à tester reste déterminante, même si cette faute est peu probable (ici moins de 1% des circuits défectueux). Si les études de pire cas s'avèrent être très pessimistes [Fedi 86] c'est d'une part parce qu'elles ne tiennent compte que d'une faute, la plus difficile à tester, mais c'est aussi parceque souvent la probabilité minimum de test est majorée grossièrement (la faute la plus difficile à tester est détectée par au moins une séquence de deux vecteurs d'entrée par exemple).

□

L'étude que nous venons de développer nous permet de travailler sur une partition plus

efficace de l'ensemble de fautes prescrit car on connait maintenant exactement la probabilité de test et la probabilité d'occurrence de presque toutes les fautes plus difficiles à tester que la RAM. Seules les fautes de transistor collé ouvert dans l'UAL testées par au moins 16 séquences d'entrée ne sont que partiellement identifiées.

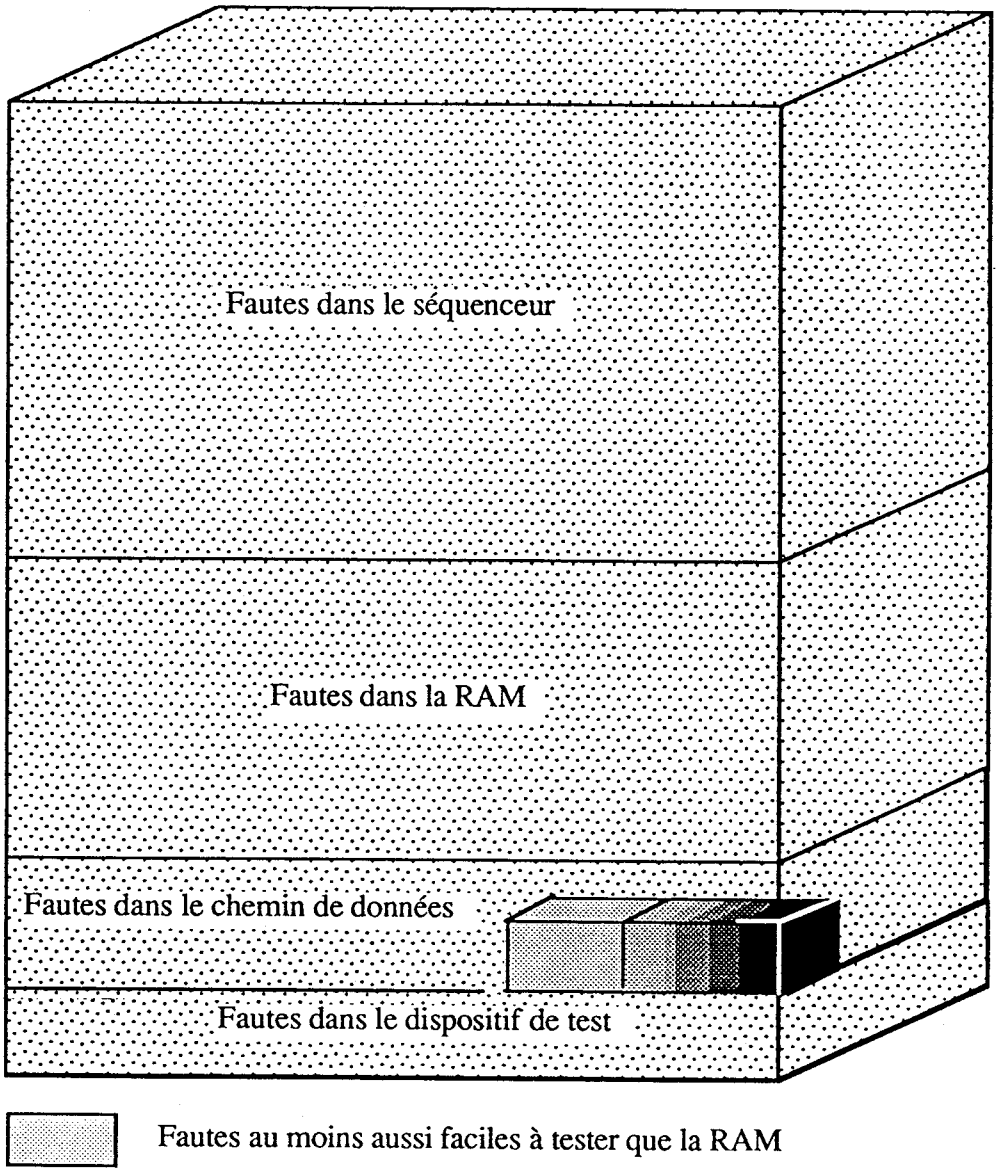


Figure 7.3 : Répartition des fautes difficiles à tester

Partition de l'ensemble de fautes:

Soit $\rho = \{F_1, F_2, F_3, F_4, F_5, F_6, F_7\}$ telle que :

F_1 = {fautes au moins aussi faciles à tester que la RAM}

F_2 = {collages ouverts des transistors sensibles de l'UAL testés par au moins 48 séquences}

F_3= {collages ouverts des transistors sensibles de l'UAL testés par au moins 16 séquences}
F_4 = {collages ouverts des transistors sensibles de l'UAL testés 12 séquences}
F_5 = {collages ouverts des transistors sensibles de l'UAL testés 8 séquences}
F_6= {collages ouverts des transistors sensibles de l'UAL testés 4 séquences}
F_7 = {collages ouverts des transistors sensibles de l'UAL testés 2 séquences}

Probabilités d'occurrence des blocs :

A partir du nombre de transistors testés par k séquences de deux vecteurs d'entrée (équations (7.5)) on peut calculer :

$$\Pr[F_1/F] = 1 - 0{,}0667 \times 0{,}3636 \times \frac{46}{120} = 0{,}990703$$

$$\Pr[F_2/F] = 0{,}0667 \times 0{,}3636 \times \frac{14}{120} = 2{,}83\ 10^{-3}$$

$$\Pr[F_3/F] = 0{,}0667 \times 0{,}3636 \times \frac{8}{120} = 1{,}62\ .10^{-3}$$

$$\Pr[F_4/F] = 0{,}0667 \times 0{,}3636 \times \frac{1}{120} = 0{,}202\ .10^{-3}$$

$$\Pr[F_5/F] = 0{,}0667 \times 0{,}3636 \times \frac{9}{120} = 1{,}82\ .10^{-3}$$

$$\Pr[F_6/F] = 0{,}0667 \times 0{,}3636 \times \frac{6}{120} = 1{,}21\ .10^{-3}$$

$$\Pr[F_7/F] = 0{,}0667 \times 0{,}3636 \times \frac{8}{120} = 1{,}62\ 10^{-3}$$

Ces différentes probabilités sont illustrées à la figure 7.3.

A partir des probabilités d'occurrence et du nombre de séquences de deux vecteurs d'entrée qui testent les fautes de chaque bloc on peut calculer $P_w(\rho)$.

Pour $P_w(\rho) = 0{,}999$ on trouve **L = 1 100 000 cycles.**

L'étude détaillée des seuls transistors sensibles dans une tranche de l'UAL, en fait 46 transistors sur 2 000 dans l'UAL (46 sur 30 000 dans tout le circuit), nous a permis de **diviser la longueur de test par 15.**

f - Bornes de P_a

Les probabilités de test et d'occurrence de toutes les fautes qui ont une probabilité de test par un vecteur inférieure à $68{,}8 . 10^{-7}$ sont exactement connues (c'est-à-dire toutes les fautes de transistors sensibles collés ouverts dans l'UAL testées par moins de 16 séquences de deux vecteurs

d'entrée). En d'autres termes on a :

$$\mathbf{P_a\ (F_k) = P_m\ (F_k)} \qquad \textbf{pour tout k = 4, 5, 6, 7.}$$

On peut donc majorer P_a de la façon suivante :

$$P_a < Pr\ [F_1'/F] + Pr\ [F_4/F]\ P_a\ (F_4) + Pr\ [F_5/F]\ P_a\ (F_5) + Pr\ [F_6/F]\ P_a\ (F_6) + Pr\ [F_7/F]\ P_a\ (F_7) \qquad (7.6)$$

avec F_1' l'ensemble de toutes les fautes qui ont une probabilité de test supérieure ou égale à $68{,}8\ 10^{-7}$.

A partir de $P_w\ (\rho)$, de l'équation (7.6) et pour une longueur de test donnée on peut calculer deux bornes de P_a qui sont très proches l'une de l'autre. Pour L = 1 100 000 cycles on a :

$$\mathbf{0{,}999\ 07 < P_a < 0{,}999\ 15}$$

Réciproquement pour $P_a = 0{,}999$ on calcule deux bornes de L :

$$\mathbf{968\ 100 < L_{MTI} < 1\ 062\ 400}$$

L'approche qui consiste à faire plusieurs études de pire cas sur des sous-ensembles de F nous permet de calculer $\mathbf{P_a}$ **à** $\mathbf{10^{-5}}$ près sous réserve de certaines hypothèses et approximations.

7 . 3 . 2 . Confiance dans l'analyse de signature

Après avoir étudié la capacité de la séquence de test à détecter un circuit défectueux nous allons mesurer la perte de confiance due au compactage de la réponse. Nous montrerons en particulier que pour les fautes difficiles à tester, l'analyseur de signature est **70 fois plus "sûr"** que la séquence de test ($1 - P_m \approx 70\ (1 - P_{Am})$). Nous calculerons la probabilité minimum de non-masquage P_{Am} du registre de signature ; puis après avoir souligné le problème qui se pose pour les faibles longueurs de test nous calculerons la probabilité minimum pondérée de détection $^*P_w\ (\rho)$.

a - Probabilité minimum de non-masquage

Comme nous l'avons vu au chapitre 5 (équation (5.9)) pour toute faute f_i de F on a :

$$Q_A(f_i) = 1 - P_A(f_i) = \frac{Pr[A_i = A_0] - Pr[Z_i = Z_0]}{Pr[Z_i \neq Z_0]}$$

et

$$P_{Am} = \min(P_A(f_1), ..., P_A(f_M))$$
$$= 1 - \max(Q_A(f_1), ..., Q_A(f_M))$$

Pour calculer P_{Am} il s'agit donc de trouver le maximum des probabilités, $Q_A(f_i)$, de masquage des fautes f_i. Pour un circuit dont le nombre de sorties est inférieur ou égal au nombre de bascules du registre de signature, il existe une connexion des sorties au registre plus sûre que la concaténation de plusieurs signatures [David 86]. Le registre de signature du MTI a été conçu de façon à maximaliser la probabilité de non-masquage. Compte tenu de ces remarques, on peut estimer le maximum de $Q_A(f_i)$ à partir de l'équation (5.10) qui est exacte pour un registre rebouclé (seule la sortie de la dernière bascule est ramenée en entrée du registre de signature) :

$$Q_A(f_i) = \frac{2^{-k}(1 + (1 - 2d_i)^a)^b(1 + (1 - 2d_i)^{a+1})^{k-b} - (1 - d_i)^L}{1 - (1 - d_i)^L}$$

dans laquelle d représente la probabilité de test par un vecteur de la faute f_i et :

$$a = \left\lfloor \frac{L}{k} \right\rfloor \quad \text{et} \quad b = k(a + 1) - L$$

Lorsque d est grand, c'est-à-dire pour les fautes faciles à tester on a :

$$Pr[Z = Z_0] \underset{d \to 1}{\to} 0$$

D'où

$$Q_A(f) \underset{d \to 1}{\to} Pr[A = A_0] \qquad (7.7)$$

On a de plus :

$$Q_A(f) \leq Pr[A = A_0] \qquad (7.8)$$

et $Pr[A = A_0]$ est une fonction décroissante de d.

On peut donc conclure, à partir des équations (7.7) et (7.8), qu'il suffit d'étudier les fautes difficiles à tester pour trouver le maximum de $Q_A(f)$.

La figure 7.4 représente la probabilité de masquage, Q_A, en fonction de la probabilité de test par un vecteur, d, pour un registre de 61 bascules et une longueur de test de 16 000 000 cycles.

On voit sur cette courbe que pour les fautes très difficiles à tester (d petit) la probabilité de masquage passe par un maximum. La faute la plus difficile à observer est celle dont la probabilité de test par un vecteur correspond à ce maximum ; ce n'est pas la faute la plus difficile à tester.

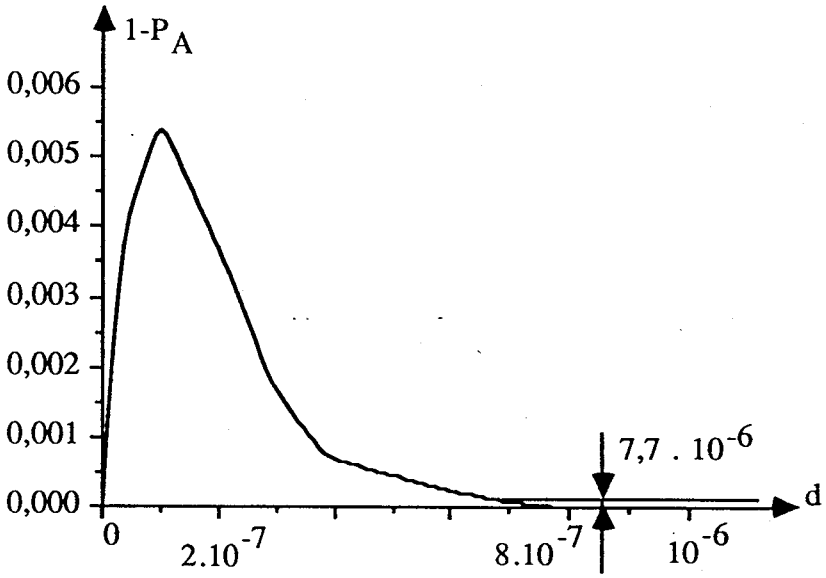


Figure 7.4 : Probabilité de masquage pour
L = 16 000 000 cycles et k = 61

Pour les fautes qui peuvent affecter le circuit MTI ($d \geq 8{,}6\ 10^{-7}$) on a :

$$Q_A(f) \leq 7{,}7\ 10^{-6}$$

D'où pour **L = 16 000 000** cycles on a :

$$\mathbf{P_{Am} = 0{,}999\ 992\ 3 \quad et \quad P_a \geq 0{,}999\ 991\ 9}$$

D'où

$$\mathbf{{}^*P_a \geq 0{,}999\ 98}$$

La perte de confiance due à l'analyse de signature est de 8.10^{-6}, soit moins de *un centième* de la perte autorisée ($100 \times 8\ .\ 10^{-6} < 10^{-3}$).

b - Influence de la longueur de test

Comme le montre la figure 7.4 pour les fautes très difficiles à tester (d petit) la probabilité de masquer une faute n'est pas une fonction monotone de la probabilité de test de cette faute. Nous avons montré expérimentalement que lorsque la longueur de test diminue le maximum

de Q_A se déplace vers la droite (figure 7.5). Aussi on a :

1) pour une faute donnée (d donné), la probabilité de masquer cette faute augmente lorsque la longueur de test diminue.

2) pour un ensemble de fautes donné, la faute la plus difficile à observer n'est pas forcément la faute la plus difficile à tester ; ceci dépend de la longueur de test.

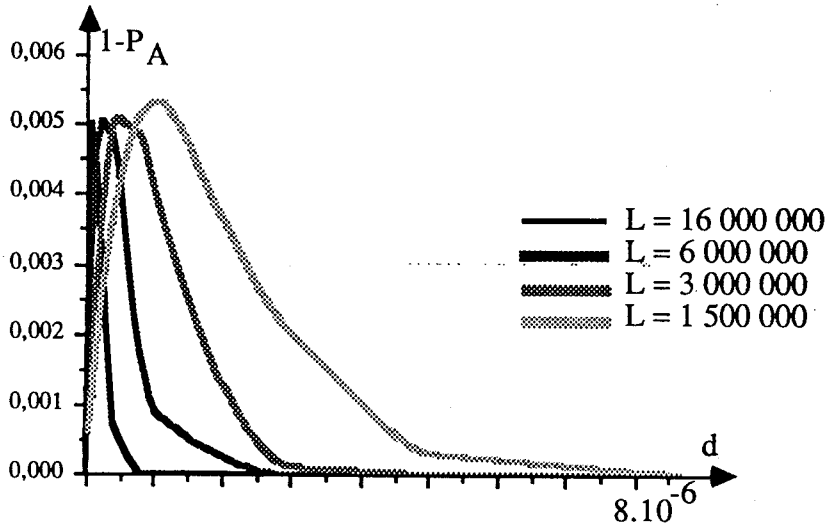


Figure 7.5 : Influence de la longueur de test

En d'autres termes lorsque la longueur de test diminue la probabilité minimum de non-masquage augmente et ce minimum ne correspond pas forcément à une faute de F. La courbe obtenue pour L = 1 100 000 cycles illustre ce phénomène (figure 7.6).

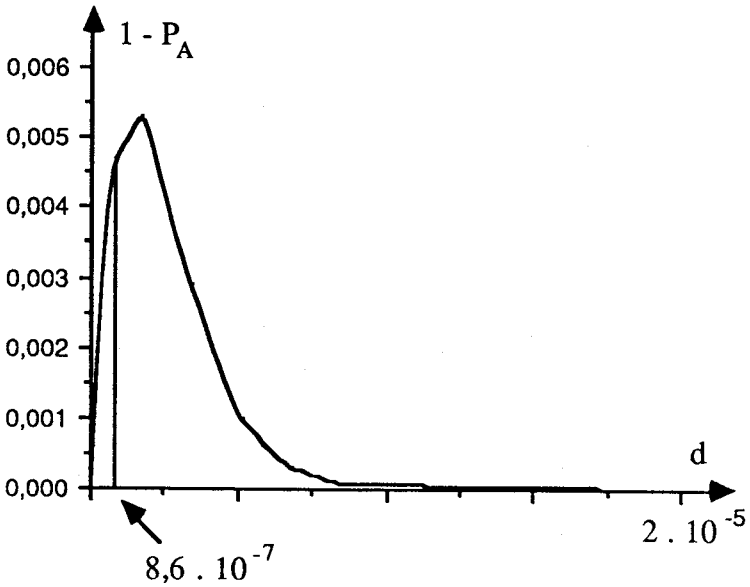


Figure 7.6 : Probabilité de masquage
L = 1 100 000 cycles

La probabilité minimum de non-masquage est obtenue pour $d = 2.10^{-6}$. On a alors pour **L = 1 100 000 cycles :**

$$\mathbf{P_{Am} = 0{,}994\ 7 \quad et \quad P_a \geq 0{,}999\ 073}$$

D'où

$$\mathbf{{}^*P_a \geq 0{,}993\ 8}$$

Soit une perte de confiance de $5{,}7\ 10^{-3}$ dûe à l'analyse de signature. On voit que lorsque la longueur de test est faible par rapport à la difficulté de test du circuit ($P_m = 0{,}612$) alors la performance de l'analyseur de signature ne peut plus être estimée grossièrement à l'aide de P_{Am}. On remarquera toutefois que la confiance dans l'analyseur de signature est toujours **70 fois** plus grande que la confiance dans le séquence de test ($1 - P_m \approx 70\ (1 - P_{Am})$).

c - Probabilité minimum pondérée de détection

Le but de notre étude n'est pas d'estimer au mieux la performance de l'analyseur de signature mais de mesurer la confiance dans la méthode de test. L'étude détaillée des fautes les plus difficiles à tester dans le circuit MTI permet d'estimer la couverture des circuits défectueux après signature à l'aide de la probabilité minimum pondérée de détection, c'est pourquoi nous ne développerons pas la mesure précise de la confiance dans l'analyseur de signature.

Pour la partition $\rho = \{F_1, F_2, F_3, F_4, F_5, F_6, F_7\}$ définie au paragraphe 7.3.1b on peut calculer les différentes probabilités répertoriées à la figure 7.7.

	$Pr[F_i/F]$ x 10^{-3}	min d_i x 10^{-7}	$P_m(F_i)$	$P_{Am}(F_i)$
F_1	990,70	86	0,99992	0,99992
F_2	2,83	206,4	1	1
F_3	1,62	68,8	0,9995	0,9997
F_4	0,202	51,6	0,9966	0,9990
F_5	1,82	34,4	0,9773	0,9971
F_6	1,21	17,2	0,8492	0,9947
F_7	1,62	8,6	0,6117	0,9953

Figure 7.7 : Données pour estimer ${}^*P_w(\rho)$
L = 1 100 000 cycles

A partir de la définition 5.8 et de la propriété 5.4 on peut minorer $*P_w(\rho)$. Les valeurs de la figure 7.7 permettent de calculer :

$$*P_w(\rho) \geq 0{,}998\ 97$$

L'analyse de signature conduit à une **perte** de confiance $3 \cdot 10^{-5}$.

Réciproquement pour L = 1 150 000 cycles on trouve les probabilités données à la figure 7.8.

Ces probabilités permettent de calculer :

$$*P_w(\rho) \geq 0{,}999\ 05$$

Une **augmentation** de moins de **5%** de la **longueur de test** calculée pour l'observation directe de la sortie permet d'assurer le niveau de confiance exigé.

	$Pr[F_i/F] \times 10^{-3}$	$\min d_i \times 10^{-7}$	$P_m(F_i)$	$P_{Am}(F_i)$
F_1	990,70	86	0,99995	0,99993
F_2	2,83	206,4	1	1
F_3	1,62	68,8	0,9996	0,9997
F_4	0,202	51,6	0,9973	0,9991
F_5	1,82	34,4	0,9808	0,9973
F_6	1,21	17,2	0,8616	0,9948
F_7	1,62	8,6	0,6280	0,9952

Figure 7.8 : Données pour estimer $*P_w(\rho)$
L = 1 150 000 cycles

L'étude de la confiance dans le test du microprocesseur MTI développée dans ce chapitre montre que l'approche proposée au chapitre 4 de ce mémoire permet d'estimer très précisément, à 10^{-5} près, la couverture des circuits défectueux. Ce résultat s'appuie sur l'analyse de 46 fautes seulement. On peut souligner, de plus, l'importance du critère de confiance retenu pour calculer la longueur de test à appliquer. En effet la probabilité minimum pondérée de test a conduit, pour cet exemple, à une réduction d'un quart de la longueur de test calculée pour $P_m = 0{,}999$, et ce à partir de la seule information nécessaire en pratique pour calculer la probabilté minimum de test.

En ce qui concerne l'analyse de signature, cet exemple montre que l'analyseur de signature est 70 fois plus sûr que la séquence de test. Néanmoins une étude grossière de la confiance dans l'analyseur de signature peut s'avérer être insuffisante. En particulier lorsque les

fautes sont difficiles à tester et que la longueur de test est faible, la faute la plus difficile à tester n'est pas forcément la faute la plus difficile à détecter. La probabilité de masquage d'une faute en fonction de la probabilité de test par un vecteur de cette faute passe par un maximum qui ne correspond pas toujours à une faute dans le circuit. La probabilité minimum de non-masquage est, dans ce cas, une mesure très pessimiste de la confiance dans l'analyseur de signature.

Nous nous sommes attachés dans ce chapitre à estimer la longueur de test aléatoire à appliquer au circuit MTI pour qu'un circuit défectueux sur mille au plus passe le test. La nouvelle approche d'estimation de la confiance dans la séquence de test que nous avons introduite au chapitre 4 de ce mémoire nous a permis de calculer deux bornes de la longueur de test qui sont très proches l'une de l'autre. Par ailleurs nous montrons à travers cet exemple que, bien qu'elle soit plus performante que la séquence de test, l'analyse de signature entraine une perte de confiance qui ne peut être estimée de façon trop grossière.

Chapitre 8

Conclusion

La plupart des chercheurs qui travaillent sur le test des circuits digitaux développent des méthodes de test de plus en plus performantes. Chacun mesure la performance de sa méthode à sa façon, bien que tous utilisent les mêmes notions de base. Le travail présenté dans ce mémoire s'appuie sur la définition de différents critères qui permettent d'estimer la qualité d'une expérience de test. Six mesures, dont une est nouvelle, sont définies avec le même *formalisme*. Cette homogénéisation nous a permis de *comparer* les différentes mesures. Parmi les mesures de la confiance dans les circuits testés, la confiance moyenne dans les circuits passés après signature,$^*C_a$, nous paraît être la mesure la plus significative pour l'utilisateur des circuits testés car elle correspond aux circuits qu'il va utiliser. Cependant la confiance moyenne dans les circuits testés après signature,$^*C_t$, est une mesure intéressante si certains circuits bons ne passent pas le test notamment.

Nous avons montré de plus que l'analyse de signature ne limite pas la confiance dans le test, c'est-à-dire que l'analyseur de signature peut être tel que $^*C_a$ *soit aussi près que l'on veut. de* C_a (la confiance moyenne dans les circuits passés). Il s'ensuit que le paramètre qui détermine la confiance dans les circuits testés est la *couverture des circuits défectueux*, P_a. Cette mesure est difficile à obtenir. L'étude comparative des différentes mesures de la confiance dans la séquence de test a permis de montrer que seule la probabilité minimum de test, P_m, est une borne inférieure de P_a facile à obtenir. La probabilité minimum pondérée de test, P_w (ρ), est une *nouvelle approche* qui permet d'estimer P_a avec une très bonne précision en calculant plusieurs P_m sur des sous-ensembles de F. Il suffit pour cela d'identifier les quelques fautes les plus difficiles à tester dans le circuit et d'estimer leur probabilité d'occurrence. Cette approche permet de tirer parti de toute l'information que l'on a sur le circuit. En d'autres termes, à partir des calculs qui sont nécessaires pour trouver la faute la plus difficile à tester, et en utilisant P_w (ρ) comme critère de confiance au lieu de P_m, on obtient une estimation plus précise de la confiance dans la séquence de test. L'application de ce principe au microprocesseur MTI a permis de *réduire d'un tiers* la longueur de test calculée pour $P_m = 0{,}999$.

L'analyse des fautes les plus difficiles à tester dans un circuit CMOS que nous avons développée afin d'estimer la probabilité d'occurrence de ces fautes a conduit au résultat suivant : toutes les fautes de transistor collé ouvert dans un circuit CMOS ne sont pas plus difficiles à tester qu'un collage classique. Seuls les transistors *sensibles* à une faute de collage ouvert nécessitent une séquence de deux vecteurs d'entrée pour être détectés. Nous avons montré de plus que le *test par mesure de courant* permet de détecter, entre autres, les collages ouverts pour lesquels un test logique n'est pas toujours possible. Enfin il s'est avéré que dans le circuit MTI toutes les fautes de

transistor sensible collé ouvert étaient détectées par *au moins deux séquences* de deux vecteurs d'entrée.

Les différents résultats obtenus sur le test des transistors collés ouverts (sensiblité, nombre de séquences de test) montrent qu'en réalité très peu de transistors collés ouverts sont testés par une seule séquence de deux vecteurs d'entrée. La probabilité minimum pondérée de test est une approche qui permet de prendre en compte cette réalité. Nous avons ainsi pu montrer qu'une longueur de test *15 fois inférieure* à celle préalablement calculée suffisait à assurer la qualité de test exigée, nous avons également pu calculer P_a à 10^{-5} *près* , sous réserve de certaines hypothèses.

L'étude que nous avons développée a permis de mettre en évidence l'influence de différents paramètres : le rendement de fabrication, la probabilité de test de chaque faute, la probabilité d'occurrence de chaque faute et l'analyseur de signature. Les résultats obtenus s'appliquent à tout circuit, tout ensemble de fautes prescrit, toute séquence de test (déterministe, aléatoire) et tout observateur (analyseur de signature, test compact statistique). Il reste cependant un point important à étudier : l'*influence des hypothèses de fautes*. En effet, dans tout ce qui a été fait jusqu'ici on suppose que l'ensemble des fautes qui peuvent affecter le circuit est connu. C'est-à-dire que l'ensemble de fautes prescrit F, correspond réellement aux fautes qui peuvent se produire. Pour un circuit réel, on ne sait pas vraiment les fautes qui peuvent se produire. L'ensemble prescrit ne correspond qu'à un modèle, qui est plus ou moins proche de la réalité. Si l'ensemble des fautes possibles F' est différent de l'ensemble prescrit F, quelle est la sensibilité de la confiance dans la méthode de test à l'écart entre F et F'? C'est le problème que nous allons chercher à aborder prochainement.

Références

AUTORISATION de SOUTENANCE

VU les dispositions de l'article 15 Titre III de l'arrêté du 5 juillet 1984 relatif aux études doctorales

VU les rapports de présentation de

. Monsieur GERBER Roland

. Madame THEVENOD Pascale

Madame DANCET Mireille, épouse JACOMINO

est autorisé(e) à présenter une thèse en soutenance en vue de l'obtention du diplôme de DOCTEUR de L'INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE, spécialité **" Automatique et Traitement du Signal "**

Fait à Grenoble, le 6 février 1989

Pour le Président de l'I.N.P.-G.
et par délégation,
le Vice-Président
P. VENNEREAU

Index

Chapitre 2

[Agrawal 82] V.D. Agrawal, M.R. Mercer : *Testability Measures - What Do They Tell Us ?* ; Conférence internationale "IEEE Test Conference", 1982, 391-396.

[Anderson 73] D.A. Anderson, G. Metze : *Design of totally Self-Checking circuits for m-out-of-n Codes* ; IEEE Transaction on Computers, C-22 n°3, mars 1973, 263-269.

[David 79a] R. David, P. Thevenod-Fosse : *Panorama des méthodes de test non déterministes*; RAIRO Automatique / Systems Ana lysis and Control, Vol 13 n°1, 1979, 5-38.

[David 79b] R. David, P. Thevenod-Fosse : *Design of Totally Self-Checking Asynchronous Circuits* ; design Automation and Fault Tolerant Computing, 1978, 271-287.

[Mc Cluskey 81] E.J. McClusckey, S. Bozorgui-Nesbat : *Design for Autonomous Test* ; IEEE Transaction on Circuits and Systems, Cas-28 n°11, novembre 1981, 1070-1079.

[Nicolaidis 86] M. Nicolaidis : *An Unified Built In Self-Test Scheme : UBIST* ; Conférence Internationale "ESSCIRC 86", Delft 1986, 173-175.

[Keiner 77] W. Keiner, R. West : *Testability Measures* ; Autotestcon, 1977, 49-55.

[Rault 71] J-C. Rault : *A Graph Theoritical and Probabilistic Approach to the Fault Detection of Digital Circuits* ; Conférence Internationale "Fault Tolerant Computing Symposium", Pasadena, juin 1971, 26-29.

[Robinson 87] J.P. Robinson, N.R. Saxena : *"A Unified View of Test Compression Methods"*, IEEE transactions on Computers, Vol C-36, n° 1, pp94-99, Janvier 1987.

[Savir 83] J. Savir : *Good controllability and Observability do not garantee Good Testability* ; IEEE Transaction on Computers, C-32 n°12, décembre 1983, 1198-1200.

[Williams 82] T.W Williams, K.P. Parker : *"Design for Testability - A Survey"*, IEEE Transactions on Computers, Vol C-31, n°1 Janvier 1982.

Chapitre 3

[David 76] R. David, G. Blanchet : *About random Fault-Detection of combinational Networks* ; IEEE Transaction on Computers, C-25, juin 1976, 659-664.

[Malaiya 84] Y.K. Malaiya, S. Yang : *The Coverage Problem for Random Testing* ; Conférence Internationale "International Test Conference", , 1984, 237-245.

[Rault 71] J-C. Rault : *A Graph Theoritical and Probabilistic Approach to the Fault Detection of Digital Circuits* ; Conférence Internationale "Fault Tolerant Computing Symposium", Pasadena, juin 1971, 26-29.

[Savir 84] J. Savir, P.H. Bardell : *On Random Pattern Test Length* ; IEEE Transactions on

Computers, C-33 n°6, juin 1984, 467-474.

[Shedletsky 77] J.J. Shedletsky : *Random Testing : Practicality vs Verified Effectiveness* ; Conférence Internationale "Fault-Tolerant Computing Symposium", Los Angeles, 1977, 175-179.

[Tellez 74] R. Tellez, R. David : *Random Fault-Detection in Logical Networks* ; Conférence Internationale "International Symposium on Discrete Systems Dig.", Zinatne, Riga (URSS), septembre 1974, 232-241.

[Wagner 87] K. Wagner, C. Chin, E.J. McCluskey : *Pseudorandom Testing* ; IEEE Transactions on Computers, C-36 n°3, mars 1987, 332-343.

[Williams 81] T.W. Williams, N.C. Brown : *Defect Level as a Function of fault Coverage* ; IEEE Transactions on computers, C-30 n°12, décembre 1981, 987-988.

Chapitre 4

[Breuer 76] M. A. Breuer, A. D. Friedman : *Diagnosis and Reliable Design of Digital Systems*; Computer Science Press,Rockville 1976.

[Hartmanis 66] J. Hartmanis, R.E. Streams : *Algebraic Structure Theory of sequential Machines;* Prentice-Hall, Londres 1966.

[Malaiya 84] Y.K. Malaiya, S. Yang : *The Coverage Problem for Random Testing* ; Conférence Internationale "International Test Conference", , 1984, 237-245.

[Shedletsky 77] J.J. Shedletsky : *Random Testing : Practicality vs Verified Effectiveness* ; Conférence Internationale "Fault-Tolerant Computing Symposium", Los Angeles, 1977, 175-179.

[Wagner 87] K. Wagner, C. Chin, E.J. McCluskey : *Pseudorandom Testing* ; IEEE Transactions on Computers, C-36 n°3, mars 1987, 332-343.

Chapitre 5

[Agrawal 83] V.K. Agrawal : *Increasing Effectiveness of Built-In-Testing by Output Data Modification* ; Conférence Internationale "FTCS-13", juin 1983, 227-234.

[David 80] R. David : *Testing by Feedback Shift Register* ; IEEE Transaction on Computers, C-29, juillet 1980, 668-673.

[David 85] R . David : *Survey of Compact Testing by Means of Signature Analysis* ; Conférence Internationale "FTSD 85", Katowice, septembre 1985.

[David 86] R. David : *Signature Analysis for Multiple-Output Circuits* ; IEEE Transaction on Computers, C-35 n°9, septembre 1986, 830-837.

[David 87] R. David : *Comments on Signature Analysis for Multiple Output Circuits* ; A paraître dans IEEE Transactions on Computers.

[Frohwerk 77] R.A. Frohwerk : *Signature Analysis : A New Digital Field Sercvice Method* ; Hewlett-Packard Journal, mai 1977, 2-8.

[Fujiwara 78] H. Fujiwara, K. Kinoshita : *Testing Logic Circuits with Compressed Data* ; Conférence Internationale "FTCS-8", Toulouser, juin 1978, 108-113.

[Hassan 84] S.Z. Hassan, E.J. McCluskey : *Increased Fault Coverage through Multiple Signatures* ; IEEE Transaction on Computers, x, 1984, 354-359.

[Hayes 76] J.P. Hayes : *Transition Count Testing of Combinational Circuits* ; IEEE Transaction on Computers, C-25, juin 1976, 613-620.

[Miller 84] D.M. Miller, J.C. Muzio : *Spectral Fault Signatures for Single Stuck-at Faults in Combinational networks* ; IEEE Transactions on Computers, C-33, août 1984, 765-769.

[Parker 76] K.P. Parker : *Compact Testing : Testing with Compressed Data* ; Conférence Internationale "FTCS-6", Pittsburgh, juin 1976, 93-98.

[Savir 80] J. Savir : *Syndrome Testable Design of Combinational Circuits* ; IEEE Transaction on Computers, C-27 n°9, juin 1980, 442-550.

[Smith 80] J.E. Smith : *Measures of the Effectiveness of Fault Signature Analysis* ; IEEE Transaction on Computers, juin 1980, 510-514.

[Susskind 83] A. K. Susskind : *Testing by Verifying Walsh Coefficients* ; IEEE Transaction on Computers, C-32, février 1983, 198-201.

[Williams 86] T.W. Williams, W. Daehn, M. Grutetzner, C.W. Starke : *Comparison of Aliasing Errors for Primitive and Non-primitive Polynomials* ; Conférence Internationale "International Test Conference", , septembre 1986, 282-288.

Chapitre 6

[Acken 83] J.M. Acken : *Testing for Bridging Faults (Shorts) in CMOS Circuits* ; 20ième Conférence IEEE Design Automation , 1983, papier 45.4, 717-718.

[Banerjee 82] P. Banerjee, J.A. Abraham : *Fault Characterization of VLSI MOS Circuits* ; IEEE International Conference on Circuits and Computers, New York, Septembre 1982 564-568.

[Baschiera 84] D. Baschiera, B. Courtois : *Testing CMOS : a Challenge* ; VLSI Design, Octobre 1984.

[Baschiera 86] D. Baschiera : *Modélisation de pannes et méthodes de test de circuits intégrés CMOS* ; Thèse de doctorat de l'Institut National Polytechnique de Grenoble, spécialité Informatique, Mars 1986.

[Brzozowski 86] J.A. Brzozowski : *Testability of CMOS Cells* ; workshop "Design for Testability", Vail (Co), Avril 1986.

[Chandramouli 83] R. Chandramouli : *On Testing Stuck Open Faults* ; IEEE Transaction on Computers, 1983, 258-265.

[David 88] R. David, S. Rahal, J-L. Rainard : *Relation between Delay Testing and Stuck-Open Testing in CMOS Circuits* ; Note Interne L.A.G n°88-77.

[Elziq 81] Y.M. Elziq : *Automatis test Generation for Stuck Open Faults in CMOS VLSI* ; Conférence Internationale IEEE "18ème Design Automation", 1981, 347-354.

[Galiay 80] J. Galiay, Y. Crouset, M. Vergniault : *Physical versus Logical Models in MOS LSI Circuits* ; IEEE Transaction on Computers,C-29 n°6, juin 1980, 527-531.

[Genda 84] J.H. Genda : *A better Anderstanding of CMOS Latch-Up* ; IEEE Transaction on Electronic Devices, ED-31 n°1, janvier 1984, 62-67.

[Jacomino 86] M. Jacomino : "Test des circuits CMOS, le circuit MTI", rapport de DEA Automatique et Traitement du Signal, Ecole Nationale d'Ingénieurs Electriciens de Grenoble, Septembre 1986.

[Jacomino 87] M. Jacomino, J-L. Rainard, R. DAVID : *Fault Detection in CMOS Circuits by Consumption Measurement* ; Conférence Internationale "FTC-Systems-3", Bremerhaven, Septembre 1987, 83-94.

[Jha 84] N.K. Jha, J.A. Abraham : *Totally Self-Checking MOS Circuits under Realistic Physical Failures* ; IEEE International Conference on Computer Design, New York, Octobre 1984, 665-670.

[Levi 81] M.W. Levi, *CMOS is Most Testable* ; Conférence Internationale "International Test Conference", 1981, papier 9.3, 217-220.

[Mead 79] C. Mead, L. Conway : *Introduction to VLSI Systems* ; Editions Addison Wesley, 1979.

[Mei 74] K.C.Y. MEI : *Bridging and Stuck-at Faults* ; IEEE Transaction on Computers, C-23, juin 1974, 42-49.

[Reddy 83] S. M. Reddy, M.K. Reddy, J.G. Kuhl : *On Testable Design for CMOS Logic Circuits* ; Conférence Internationale "International Test Conference", 1983, papier 15.2, 35-445.

[Reddy 86] S.M. Reddy, M.K. Reddy : *Testable Realizations for FET Stuck Open Faults in CMOS Combinational Logic Circuits* ; IEEE Trancastion on Computers, C-35 n°8, août 1986,742-754.

[Sastry 88] S. Sastry, M. Breuer : *Detectability of CMOS Stuck Open Faults Using Random and Pseudorandom Test Sequences* ; IEEE Transaction on Computers, C-7 n°9, septembre 1988, 933-945

[Thorel 87a] P. Thorel : *Contribution au test autonome des circuits VLSI : Un microprocesseur à test aléatoire intégré* ; Thèse de doctorat de l'Institut National Polytechnique de Grenoble, spécialité Automatique et Traitement du Signal, Juillet 1987.

[Wadsack 78] R.L. Wadsack : *Faults Modeling and Logic Simulation of CMOS and MOS Integrated Circuits* ; The Bell System Technical Journal, Vol 57, N°5, Mai 1978.

[Woodhall 86] B.W. Woodhall, B.D. Newman, A.G. Sammuli : *Emperical Results on Undetected CMOS Stuck-open Faults* ; VAIL 1986.

Chapitre 7

[David 86] R. David : *Signature Analysis lor Multiple-Ouput Circuits* ; IEEE Transaction on Computers, C-35 n°9, septembre 1986, 830-837.

[Fedi 86] X . Fedi, R . David : *Some Experimental Results from Random Testing of Microprocessors* ; IEEE Transactions on Instrumentation and Measurement,IM-35, mars 1986,78-86.

[Thorel 87a] P. Thorel : *Contribution au test autonome des circuits VLSI : un microprocesseur à test intégré* ; Thèse de Doctorat de l'Institut national Polytechnique de Grenoble, spécialité Automatique, juillet 1987.

[Thorel 87b] P. Thorel, R. David, J. Pulou, J-L. Rainard : *Design for random Testability* ; Conférence Internationale "International Test conference", Washington, septembre 1987.

Index

Index