

C 1197

**THÈSE**  
pour l'obtention du  
**DOCTORAT D'ÉTAT ES SCIENCES**

Spécialité : MATHÉMATIQUES  
Mention : INFORMATIQUE

*présentée par*

**Serge MIRANDA**



**ARCHITECTURE FORMELLE**  
**D'UN SYSTÈME D'INTÉGRITÉ**  
**POUR UNE BASE DE DONNÉES RÉPARTIES**

*soutenu le 27 septembre 1980 devant la Commission composée de :*

MM. G. BAZERQUE ..... *Président*

- R. BEAUFILS
- C. BETOURNE
- E. GELENBE
- J. LE BIHAN
- G. LE LANN
- G. POPEK



*Examineurs*

## TABLE DE MATIERES

## PREFACE

## INTRODUCTION

1.	L'informatisation de la société	1
1.1.	Développement des bases de données	3
1.2.	Puissance accrue de mémorisation et de traitement	5
1.3.	Mise en oeuvre de réseaux d'ordinateurs	6
1.3.1.	Tendances de développement dans les réseaux	6
1.3.2.	Normalisation des réseaux d'ordinateurs	11
2.	Bases de données réparties	14
2.1	Avantages de l'emploi d'une BDR	14
2.2.	Approches de conception (par fragmentation ou intégration)	15
2.2.1.	Niveaux externe et conceptuel	15
2.2.2.	Niveau interne	16
2.2.3.	Niveau des chemins d'accès globaux	16
2.3.	Architecture fonctionnelle du système réparti	18
2.4.	Inventaire des principaux axes de recherche dans les BDR	20
3.	Sécurité des données	23
3.1.	Objectifs d'une base de données et sécurité des données	23
3.2.	Aspects de la sécurité des données	25
3.2.1.	La confidentialité	25
3.2.2.	L'intégrité	28
4.	Motivation et intérêt de la recherche proposée	29

5.	Plan de la thèse	29
6.	Références	33

## PARTIE 1 : MODELE DIACRITIQUE ET INTEGRITE LOCALE D'UNE BASE DE DONNEES REPARTIE

### CHAPITRE 0 : ARCHITECTURE D'UN SYSTEME D'INTEGRITE POUR UNE BASE DE DONNEES REPARTIE

1.	Transactions sur une base de données locale	1
1.1.	Définition d'une transaction	2
1.2.	Opérateurs possibles dans une transaction	3
1.3.	Gestion des transactions	3
1.4.	Système transactionnel	4
2.	Architecture d'un système d'intégrité pour une base de données répartie	5
2.1.	Besoin d'une architecture	5
2.2.	Description structurale	6
2.2.1.	Le niveau global d'intégrité	7
2.2.2.	Le niveau local d'intégrité	7
2.3.	Description fonctionnelle	8
3.	Références	10

### CHAPITRE 1 : ETUDE SYNTHETIQUE DE L'INTEGRITE D'UNE BASE DE DONNEES REPARTIE (NIVEAU LOCAL ET GLOBAL)

1.	Interférence de transactions concurrentes	1
1.1.	Notion d'interférence	2
1.2.	Anomalies d'interférence	2

1.2.1.	Anomalie de "mise à jour perdue"	3
1.2.2.	Anomalie de "lecture impropre"	4
1.2.3.	Anomalies de "lecture non reproductible" et de "lecture incohérente"	5
1.3.	Concepts attachés au contrôle de l'interférence	6
1.3.1.	Concept de sérialisation en milieu conflictuel	7
1.3.2.	Concept d'atomicité des transactions en milieu défaillant (et conflictuel)	7
1.4.	Mécanisme de résolution de l'interférence	10
1.4.1.	Mécanisme de détection/résolution de l'interférence	10
1.4.2.	Mécanismes de prévention de l'interférence	10
2.	Mécanismes de verrouillage dans les bases de données (centralisées ou réparties)	16
2.1.	Granularité de verrouillage	16
2.2.	Ordonnancement des transactions	17
2.3.	Niveaux de verrouillage	18
2.3.1.	Verrouillage de bas niveau	18
2.3.2.	Verrouillage de haut niveau	20
2.3.3.	Problème de "confusion d'identité"	22
2.4.	Classification des mécanismes de résolution de l'interblocage	23
2.4.1.	Interblocage	23
2.4.2.	Mécanismes de résolution de l'interblocage	24
3.	Références	31

## CHAPITRE 2 : MODELE DIACRITIQUE ET SOLUTION A L'INTEGRITE LOCALE D'UNE BASE DE DONNEES REPARTIE

1.	Les types de données abstraits (TDA)	1
1.1.	Que signifie la notion d'abstraction ?	1
1.2.	Qu'est-ce qu'un TDA ?	3

1.3.	En quoi le concept de TDA enrichit-il ceux de type et de module ?	6
1.4.	Quelle application des TDA peut-on envisager dans les bases de données ?	7
1.5.	Quelles sont les bases théoriques du concept de TDA ?	8
1.5.1.	Approche propositionnelle	8
1.5.2.	Approche algébrique	10
1.5.3.	Avantages et inconvénients des deux approches	16
2.	Le modèle diacritique	17
2.1.	Paradigme du modèle diacritique	17
2.2.	Panorama des recherches concernant l'intégration des TDA dans les systèmes informatiques	19
2.2.1.	TDA et systèmes opératoires	19
2.2.2.	TDA et systèmes de gestion de bases de données	19
2.3.	Support linguistique des TDA pour la formalisation d'un système d'intégrité	21
2.3.1.	Langage OBJ-O	21
2.3.2.	Exemple de spécifications algébriques : l'objet LISTE	24
3.	Définition et spécification formelle du verrouillage de moyen niveau dans une base de données centralisée	26
3.1.	Définition du verrouillage de moyen niveau	26
3.1.1.	SGBD "général"	26
3.1.2.	Chaînes de DIAM	27
3.1.3.	Comparaison du verrouillage de moyen niveau avec les verrouillages existants	30
3.2.	Spécification du verrouillage de moyen niveau	31
3.2.1.	Spécification des chaînes de DIAM	31
3.2.2.	Spécification des opérations de verrouillage de moyen niveau	43
4.	Références	47

PARTIE 2 : MODELE DIACRITIQUE ET INTEGRITE GLOBALE D'UNE  
BASE DE DONNEES REPARTIE

CHAPITRE 0 : THEOREMES D'INTEGRITE MUTUELLE

1.	Problème de synchronisation en mise à jour d'entités dupliquées	1
1.1.	Protocole de synchronisation	1
1.1.1.	Classification des mécanismes de synchronisation	3
1.1.2.	Concepts attachés au protocole de coordination inter-contrôleurs dans une BDR totalement dupliquée	5
1.2.	Atomicité de transactions dans un environnement conflictuel et/ou défaillant	11
2.	Modèle diacritique et synchronisation en mise à jour d'une BDR totalement dupliquée	15
2.1.	Formalisation d'un protocole de synchronisation	16
2.1.1.	Formalisation d'un contrôleur de synchronisation	17
2.1.2.	Spécification du parallélisme fonctionnel	21
2.2.	Théorèmes d'atomicité	22
2.2.0.	Définition d'un $\Sigma$ -homomorphisme total	22
2.2.1.	Théorème 1 d'atomicité	22
2.2.2.	Corollaire : condition suffisante de maintien de l'intégrité mutuelle	26
2.2.3.	Théorème 2 d'atomicité	27
2.2.4.	Corollaire : autre condition suffisante de maintien de l'intégrité mutuelle	28
2.3.	Théorèmes d'intégrité mutuelle forte	28
2.3.1.	Théorème 1 d'intégrité mutuelle forte (condition nécessaire et suffisante)	28
2.3.2.	Corollaire : théorème 2 d'intégrité mutuelle forte (condition suffisante)	30
2.4.	Théorèmes d'intégrité mutuelle faible	30
2.4.1.	Théorème 1 d'intégrité mutuelle faible (condition nécessaire et suffisante)	30
2.4.2.	Corollaire : théorème 2 d'intégrité mutuelle faible (condition suffisante)	32
2.5.	Indépendance vis-à-vis du protocole de synchronisation	34
3.	Références	36

CHAPITRE 1 : MODELE DIACRITIQUE ET SOLUTION ROBUSTE  
A L'INTEGRITE GLOBALE D'UNE BASE DE  
DONNEES REPARTIE

1	Présentation informelle de DLP	1
1.1.	Objectifs et hypothèse de DLP	1
1.1.1.	Objectifs poursuivis	2
1.1.2.	Hypothèse sous-jacente	5
1.2.	Description de DLP dans un environnement fiable	6
1.2.1.	Automate d'états finis	6
1.2.2.	Description de DLP pour une transaction unique	7
1.2.3.	Description de DLP pour des transactions interférentes	10
1.2.4.	Fonction de transition de l'automate décrivant le fonctionnement d'un contrôleur	15
1.2.5.	Déperdition	17
1.2.6.	Théorème de déperdition	18
1.3.	Description de DLP dans un environnement défaillant	21
1.3.1.	Analyse exhaustive des pannes	21
1.3.2.	Table des contrôleurs actifs (CTACT)	26
1.3.3.	Journal de modification totalement dupliqué	26
1.3.4.	Anneau virtuel de résilience	28
1.3.5.	Comparaison avec d'autres solutions	29
2.	Présentation formelle de DLP à l'aide du modèle diacritique	32
2.1.	Signature du TDA (SYNC) associé à un contrôleur	32
2.2.	Spécification de DLP	34
2.2.1.	Spécification de SYNC sans un langage proche d'OBJ-0	34
2.2.2.	Analyse des changements d'états	42
2.2.3.	Intégration de la robustesse	43
2.3.	Vérification de DLP	44
2.3.1.	Vérification de l'intégrité mutuelle	44
2.3.2.	Vérification de la robustesse	53

CHAPITRE 2 : MODELE DIACRITIQUE ET UNIFORMISATION  
DES PROTOCOLES DE SYNCHRONISATION  
EXISTANTS

1.	Classification des protocoles de synchronisation	1
1.1.	Stratégies avec consensus unanime (SCU)	1
1.1.1.	Anneau Virtuel de Transmission - protocole AVT - (ELLI77a), (ELLI77b)	1
1.1.2.	Anneau Virtuel de Séquencement - protocole AVS - (LELA77), (LELA78)...	2
1.1.3.	Anneau Virtuel de Résilience - protocole DLP - (MIRASO)...	2
1.2.	Stratégies avec consensus majoritaire (SCM)	2
1.3.	Stratégies avec copie primaire (SCP)	3
2.	Spécification et vérification des protocoles de synchronisation	5
2.1.	Protocole avec anneau virtuel de transmission (AVT)	5
2.1.1.	Description informelle	7
2.1.2.	Formalisation	11
2.2.	Protocole avec anneau virtuel de séquencement (AVS)	19
2.2.1.	Description informelle	19
2.2.2.	Formalisation	24
2.3.	Protocole avec consensus majoritaire (ACM)	32
2.3.1.	Description informelle	32
2.3.2.	Formalisation	38
2.4.	Protocole avec copie primaire (ACP)	46
2.4.1.	Description informelle	46
2.4.2.	Formalisation	50
3.	Comparaison synthétique des différents protocoles	59
4.	Références	63

## DISCUSSION ET PROSPECTIVES

1.	Quel est l'intérêt novateur du modèle diacritique pour la formalisation des protocoles de synchronisation ?	1
1.1.	Présentation du modèle basé sur les réseaux de NUTT	2
1.2.	Apports du modèle diacritique	7
1.2.1.	Spécification formelle	8
1.2.2.	Validation formelle	9
1.2.3.	Mesures du système opérationnel	10
1.2.4.	Implantation	10
1.2.5.	Vérification formelle	10
1.2.6.	Corrélation avec les niveaux fonctionnels adjacents	11
1.3.	Tableau comparatif des modèles existants	13
1.4.	Intérêt et limite du modèle diacritique pour la formalisation des protocoles de synchronisation	13
2.	Quels sont les perspectives du modèle diacritique ?	14
2.1.	Le modèle diacritique et les protocoles de communication	14
2.1.1.	Les modèles de transition	15
2.1.2.	Les modèles algorithmiques	15
2.1.3.	Les modèles hybrides	16
2.2.	Le modèle diacritique et l'appréhension des systèmes	16
2.3.	Recherches futures	17
3.	Références	19