# 개선된 자동정리증명기법에 기초한 유한체상의 디지털논리시스템 구성

박 춘 명*

# Construction of the Digital Logic Systems based on the Improved Automatic Theorem Proving Techniques over Finite Fields

Chun-Myoung Park*


## 요 약

본 논문에서는 개선된 자동정리증명기법에 기초하여 유한체상의 디지털논리시스템을 구성하는 방법을 제안하였다. 제안한 방법은 먼저 유한체상의 중요한 수학적 성질을 논의하였고 자동정리증명기법의 개념과 기본 성질을 서술하였다. 그리고 개선된 자동정리증명기법을 적용하기 위해 몇가지 정의를 하였으며 이를 근간으로 디지털논리시스템의 Building Block을 제안하였다. 또한, 디지털논리시스템을 구성하기 위한 중요한 관계를 정의하였으며 최종 유한체상의 디지털논리시스템을 개선된 자동정리증명기법에 의해 구성하였다.

## ABSTRACT

This paper propose the method of constructing the Digital Logic Systems based on the Improved Automatic Theorem Proving Techniques(IATP) over Finite Fields. The proposed method is as following. First, we discuss the background and the important mathematical properties for Finite Fields. Also, we discuss the concepts of the Automatic Theorem Proving Techniques(ATP) including the syntactic method and semantic method, and discuss the basic properties for the ATP. In this step, we define several definitions of the IATP, Table Pseudo Function Tab and Equal. Next, we propose the T-gate as Building Block(BB) and describe the mathematical representation for the notation of T-gate. Then we discuss the important properties for the T-gate. Also, we propose the several relationships that are Identity relationship, Constant relationship, Tautology relationship and Mod R cyclic relationship. Then we propose Mod R negation gate and the manipulation of the don't care conditions. Finally, we propose the algorithm for the constructing the method of the digital logic systems over finite fields. The proposed method is more efficiency and regularity than any other earlier methods. Then, we prospect the future research and prospects.



키워드

Finite Fields, Automatic Theorem Proving Techniques, Digital Logic Systems, Building Block etc.


## Ⅰ. 서 론

현존의 디지털논리시스템과 이를 근간으로 한 컴퓨터 하드웨어 분야는 2진(2치)논리에 바탕을 두고 많은 발전을 해왔으나 보다 복잡하고 다양한 기능을 실현하기 위해서는 좀 더 집약된 VLSI와 ULSI 칩의구성이 필요하게 되

* 충주대학교 전기 · 전자 및 정보공학부 컴퓨터공학전공

접수일자 : 2006. 6. 13

었다. 이를 해결할 수 있는 개념으로 2진논리의 확장개념을 도입하여 그 효율을 높이고 있다. 특히 최근에는 디지털논리시스템의 설계시 자동설계기법의 중요성이 점차 커지고 있으며, 이 중 자동정리증명기법을 도입한 설계기법은 상당히 효과적이며 이에 대한 기존의 연구내용들은 다음과 같다. W.C.kabat와 A.S.Wojcik[1]는 디지털논리시스템 설계시에 demodulation 개념을 도입하여 자동정리증명기법을 적용하였으며, W.C.kabat[2]는 스위칭함수의 도출에 자동정리증명기법을 적용하여 간략화된 스위칭함수를 구하였다. 그리고 W.S.Wojciechowski와 A.S.Wojcik[3]는 인공지능의 개념을 자동정리증명기법에 도입하여 좀 더 효율적으로 디지털논리시스템 구성의 한가지 방법을 제안하였다. 또한, V.J.Sanchez와 W.C.kabat[4]는 최초로 자동정리증명기법에 기초한 디지털순차논리시스템구성의 한가지 방법을 제안하였으며 D.Snyers와 A.Thayse[5]는 자동정리증명기법과 알고리즘상태머시인(Algorithmic State Machine)을 사용하여 디지털논리시스템을 구성하는 한가지 방법을 제안하였다. V.S.Stokkermans는 Non-Classical 논리에서의 정리와 표현에 대한 논의[6]와 Lattics 기반의 세만틱과 정리의 표현에 대해 논의[7]하였다. H.Ganzinger 등[8]은 확장논리에서의 자동정리증명기법에 대한 기술에 논의하였다. 이들 연구들은 각각의 특징이 있으나 크게 2가지 관계에 의한 자동정리증명기법만 효과적으로 활용하는 방안에 대한 연구가 대부분이고, 좀 더 다양한 관계에 의한 자동정리증명기법에 대한 연구는 미흡한 상태이다. 따라서 본 논문에서는 기존 논문에서의 단점을 보완하고 좀 더 일반화된 자동정리증명기법의 방법을 제안하였다.

## Ⅱ. 자동정리증명기법

디지털논리시스템설계 과정은 요구되는 함수의 기능을 수행 할 수 있는 효과적이고 최적화된 회로를 실현하는 것이다. 현재의 디지털논리시스템설계에서의 자동 툴(Automatic Tool)은 다음과 같은 조건들을 만족하여야 한다.

- 임의의 레벨 수의 논리시스템에 적응 할 수 있어야 한다.
- 임의의 논리 모듈(logic module)의 집합에 대해 수행되어야 한다.
- 이상적인 시간에 최적의 설계를 생성하여야 한다.
- 새로운 방법이나 설계의 요구에 대한 Cost가 좋아야 한다.

이러한 목적을 효과적으로 수행 할 수 있는 방법으로 최근에 자동정리증명기법(Automated Theorem Proving Technique)이 도입되고 있다. 정리증명기(Theorem prover)는 서술(statement)된 내용을 공리(axiom)로 반박(contradict)하여 최종 간략화된 함수를 도출하는 것이며, 이들 줄어든 문제는 최종 질의와 더불어 목적함수를 표현한다.

### 2.1. Syntactic 방법과 Semantic 방법

자동정리기법은 크게 Syntactic(구문) 방법과 Semantic(어의) 방법으로 나눌 수 있으며 그 각각의 특징은 다음과 같다.

■ Syntactic 방법

이 방법은 주어진 시스템의 성질에 관한 내용을 사용하는 방법이며, 공리의 집합은 해당 Building Block과 원소를 정의한다. PR은 First-Order System에서의 술어를 의미하며 절은 집합 표현에 있어서 Skolem conjunctive 형태를 이룬다.

■ Semantic 방법

이 방법은 시스템 내에 존재하는 성질을 사용하는 방법으로, 일반적인 공리의 집합은 항상 사용가능한 함수이어야 하며 쉽게 구성 할 수 있어야 한다. 목적함수에 대한 마지막 질의는 목적함수를 표현하는 PR(F( ..... )) 형태를 가져야 한다.

### 2.2. Table Pseudo Function : Tab

주어진 임의의 함수에 대한 진리치표는 의사함수 Tab(Table Pseudo Function Tab: TPF Tab)을 사용하여 표현할 수 있다.

### 2.3. EQUAL

단항함수에 대해서 다음과 같은 EQUAL Semantic을 사용하여 간략화 할 수 있다.

EQUAL(Fi(X1, X2, ..... , Xk) , Ci)

여기서, Xi는 입력 X=X(X1, X2, ..... , Xk)의 i번째 입력 벡터이고, Ci는 (X1, X2, ..... , Xk)의 i번째 순열에 대한 Fi

의 값이다. 이러한 것들을 PSF(Primitive Synthesizable Functions)라 하며, McClusky의 strong threshold literal과 같은 동작을 한다.

### 2.4. 자동정리증명기법의 기본적인 단계

자동정리기법을 도입하여 디지털논리시스템을 구현하는 단계는 일반적으로 다음과 같은 4가지 단계로 요약된다.

[STEP1] 함수진리치표의 입력

[STEP2] 요구되는 Building block을 사용하여 표준화(Canonical) 회로구조를 도출한다.

[STEP3] 정규화 Network을 간략화 한다.

[STEP4] 최종 회로를 합성한다.

특히 Demodulation은 자동정리증명기법을 수행하는 주요한 기법이다.

### 2.5. 각종 정의

Demodulation은 증명 찾기의 모든 단계에서 발생되는 자동과정이다. 이 과정을 통해 절의 공간(Clause Space)에 term을 재배치하여 효과적으로 원래의 절을 삭제할 수 있으며, 이는 곧 절의 공간을 줄일 수 있음을 의미한다.

근본적으로 간략화와 표준형의 2가지를 사용하여 다시 절의 내용을 서술할 수 있으며, 결국 최적의 디지털논리시스템의 설계를 성공적으로 수행할 수 있다. 본 눈문을 전개하는데 필요한 정의를 다음과 같이 정의한다.

[정의 1] term은 상수, 변수, 또는 함수 F(t1, t2, ..... , tn)이다. 여기서 F는 n-ary 함수이고 ti는 term이다.

[정의 2] Atom은 P(t1, t2, ..... ,tn)이다. 여기서, P는 n-ary 관계(서술)이고 ti는 term이다. 또한, Atom은 근본적으로 진(true)/위(false) 항목이다.

[정의 3] Literal은 atom이거나 atom의 부정이다.

[정의 4] 절(clause)은 literal의 Disjunction이다.

[정의 5] 절의 공간은 절의 Disjunction이다.

[정의 6] 만일 절이 다음의 조건을 만족하면 절은 등가 Unit(Equality Unit)이다.

- 정확히 한개의 literal을 포함하고 있다면 이는 Unit 절(Unit clause)이다.
- literal의 서술은 이항관계(binary relation)이다.
- 서술 명은 EQUAL이다.

## Ⅲ. Building Block 구성

최근에는 전자공학의 눈부신 발달과 이에 기초를 둔 각종 회로소자의 집적화(VLSI화 또는 ULSI화)로 인하여 개별적인 회로소자 사용보다는 특정함수 기능을 갖는 회로소자들의 묶음을 단일회로소자(Unit Circuit Device)로 취급하여 디지털논리시스템을 설계하는 경향이 두드러지고 있으며, 이때의 단일회로소자를 그 디지털논리시스템상의 Building Block(BB)이라 한다.

### 3.1. Building Block T-gate

T-gate에 대한 블록선도는 그림3-1과 같고, $TG[R]_{var\,k}$의 var은 해당 변수명(또는 level 명), k는 해당 level 에서의 k번째 T-gate를 의미한다. 그리고, 입출력에 대한 동작특성은 각각 식(3-1)과 식(3-2)와같다.

$$I_i=e_i=C_i\in GF(R)(R=P^m)\ (i=0,1,\ldots\ldots,R-1) \quad (3\text{-}1)$$

$$Output=I_i=e_i \text{ iff } C_i=i(R=P^m)(i=0,1,\ldots\ldots,R-1) \quad (3\text{-}2)$$

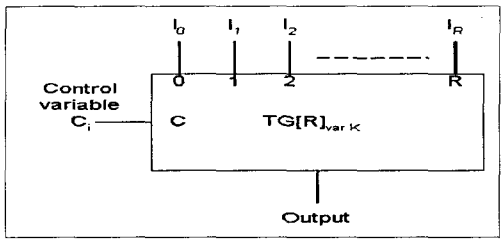


그림 3-1. Building Block T-gate의 블록선도.
Fig. 3-1. Block diagram of Building Block T-gate.

### 3.2. 수학적 표기

1) $TG[R]_{var\,k}$ : T-gate

여기서, $R=P^m$, var는 T-gate level 명, k는 k level에서의 T-gate 번호이다. 또한, k는 해당 T-gate level에서의 제어입력 이름과 동일하다.

2) $TG[R]_{var\,k}=\langle e_j\rangle$ : T-gate 의 입력을 표시함. $(j=0,1,\ldots\ldots,P^m)$

### 3.3. Building Block T-gate의 유용한 성질

■ 항등관계 (Identity Relationship)

항등관계는 임의의 조합논리디지털시스템 에 대한 함수 진리치표상에서 1)입력변수와 이 입력변수에 대응하는 출력값 사이의 관계 2)입력변수에 대응하는 값들끼리의 관계를 조사하여 이것들이 서로 항등관계가 존재 한다

면 회로를 간략화 할 수 있다.

■ 정수관계(constant Relationship)

정수관계는 어떤 입력변수의 모든 값이 같은 경우에 적용된다.

■ 중복관계 (Tautology Relationship)

이 경우는 입력이 바로 출력인 경우에 적용되며 이는 앞의 항등관계의 특별한 경우에 해당된다.

### 3.4. Building Block의 사이클릭(Cyclic) 관계

유한체상의 임의의 함수 진리치표상에서 입력변수와 이 입력변수에 대응하는 출력값 사이의 관계가 Modular R(Mod R)(단, $R=P^m$이고 P는 소수이며 m은 양의 정수) 사이클릭 조건이 존재할 때 적용된다.

■ Mod R 좌측사이클릭

Mod R 좌측사이클릭 관계는 임의의 함수 진리치표상에서 입력변수와 이 입력변수에 대응하는 출력값 사이의 관계가 Mod R 좌측 사이클릭 조건이 존재할때 적용된다. 블록선도는 다음 그림 3-2와 같고, 동작특성은 다음 식(3-3)과 같다.

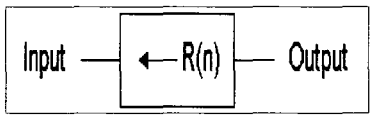


그림 3-2. Mod R 좌측사이클릭 게이트의 블록선도
Fig. 3-2. Block Diagram of Mod R left cyclic gate.

LCYLE[R(n)] (3-3)

(단, $1 \le n \le R-1$, n는 정수이고 $R=P^m$)

동작특성 : 출력은 입력을 n만큼 좌측 사이클릭시킨 값이다. 수학적 표기는 다음과 같다.

$TG[R]_{var\ k}^{\leftarrow m}$ : T-gate의 입력들을 좌측으로 n만큼 사이클릭 함. (단, $1 \le n \le R-1$, n는 정수이고 $R=P^m$)

■ Mod R 우측사이클릭

Mod R 우측사이클릭 관계는 임의의 함수 진리치표상에서 입력변수와 이 입력변수에 대응하는 출력값 사이의 관계가 Mod R 우측 사이클릭 조건이 존재할 때 적용된다. 또한, 이 Mod R 우측사이클릭 관계는 앞에서의 Mod R 좌측사이클릭 관계와 쌍대관계에 있다. 블록선도는 다음 그림 3-3와 같고, 동작특성은 다음 식(3-4)와 같다.

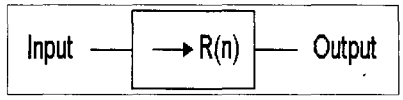


그림 3-3. Mod R 우측 사이클릭 게이트의 블럭선도.
Fig. 3-3. Block Diagram of Mod R rigth cyclic gate.

RCYCLE[R(n)] (3-4)

(단, $1 \le n \le R-1$, n는 정수이고 $R=P^m$)

동작 특성 : 출력은 입력을 n만큼 우측 cyclic 시킨 값이며 수학적 표기는 다음과 같다.

$TR[R]_{var\ k}^{\leftarrow n}$ : T-gate의 입력들을 우측으로 n만큼 cyclic 함. (단, $1 \le n \le R-1$, n는 정수이고 $R=P^m$)

### 3.5. Mod R 부정

이 관계는 1)임의의 함수 진리치표상에서 입력변수와 이에 대응하는 출력값의 관계가 Mod R 부정의 관계가 있는 경우, 2)임의의 함수 진리치표의 block 원소들간의 관계가 서로 Mod R 부정의 관계가 있을 때 적용된다. 블럭선도는 다음 그림 3-4와 같다.


그림 3-4. Mod R 부정게이트 NOT[R]의 블럭선도.
Fig. 3-4. Block Diagram for Mod R negation gate NOT[R].

여기서, $R=P^m-1$이며 P는 소수이고 m은 양의 정수임

### 3.6. 무관항 조건 "-"(Dont't care condition "-")

만일 임의의 유한체상의 진리치표상에 무관항 조건이 존재하면 이 무관항을 해당 block내의 원소들과 비교·파악하여 앞에서 논의한 각종 관계를 적용하기 좋은 원소값으로 대치하여 처리한다.

## Ⅳ. 유한체상의 디지털논리시스템 구성

### 4.1. 디지털논리시스템의 기본 성질

디지털논리시스템은 크게 조합논리시스템과 순차논리시스템으로 구분할 수 있으며 모든 디지털논리시스템의 기본은 조합논리시스템이다. 따라서 본 절에서는 디지

털논리시스템의 기본인 조합논리시스템의 기본성질에 대해 논의한다. 조합논리시스템은 출력이 입력 발생과 동시에 이루어 지는 디지털논리시스템을 의미하며, 유한체상에서의 m변수 입력, n출력의 일반적인 조합논리시스템의 블록선도는 다음 그림4-1과 같다.

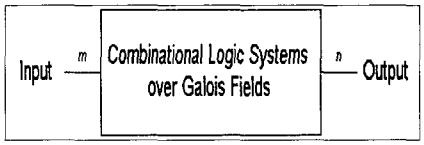


그림 4-1. 유한체상의 조합논리시스템의 블록선도.
Fig. 4-1. Block diagram of the combinational logic systems over Finite Fields.

한편, 조합논리시스템을 구성하기 위해서는 먼저 조합논리시스템에서 요구하는 기능에 대한 함수(조합논리시스템의 입력과 출력간의 관계 표현)를 도출하여야 한다. 일반적으로 이러한 함수기능에 관한 표현은 입출력간의 관계를 표로 나타내는 진리치표(Truth Table)를 참조한다. 따라서, 조합논리시스템 설계자는 해당 조합논리시스템을 회로로 실현하기 위해 진리치표로부터 함수를 구하여야 하며 가능한한 최적의 간략화된 함수(Optimal Simplification Function)를 도출하여야 한다.

### 4.2. 유한체상의 디지털논리시스템구성 알고리즘

본 절에서는 Ⅲ장에서 논의한 Building Block T-gate의 각종 관계를 적용하여 유한체상의 디지털논리시스템구성의 한가지 방법을 제안한다. 본 논문에서 제안한 함수구성 알고리즘의 절차는 다음과 같다.

[STEP1] 임의의 유한체상의 디지털논리시스템의 진리치표로부터 각 T-gate level의 제어변수를 선택한다. 특히, 1번째 level의 제어변수는 될 수 있는데로 모든 입력 $e_0, e_1, \ldots\ldots, e_{R-1}(R=P^m)$이 사이클릭 형태로 되어있는 변수를 제어변수로 선택한다.

[STEP2] 절차1에서 선택한 제어변수 별로 T-gate $TG[R]_{var\ k}$를 할당한다.

[STEP3] 절차2로부터 1번째 level의 각 T-gate $TG[R]_{var\ k}$를 Ⅳ장에서 정의한 수학적 표기로 나타낸다. 이때 1번째 level의 기본 Building Block T-gate(BTG : Basic T-gate Building Block)인 BTG는 가능한한 모든 입력 $e_0, e_1, \ldots\ldots, e_{R-1}(R=P^m)$이 순서적이거나 사이클릭 형태로 되어있는 변수를 제어변수로 설정한다

[STEP4] 1번째 level의 BTG와 Ⅳ장에서 정의한 수학적 표기 및 각종 유용한 관계를 토대로 하여 나머지 1번째 level의 각 T-gate $TG[R]_{var\ k}$를 조사하여 될 수 있는데로 BTG로 표현한다.

[STEP5] 1번째 level을 제외한 나머지 모든 level(2번째, 3번째 등의 level)에서의 각 T-gate를 절차4와 같은 방법으로 처리한다.

[STEP6] 절차4 및 절차5에서 구한 각 level에서의 Building Block T-gate로써 회로를 실현한다. 이 절차6에서 최종 유한체상의 디지털논리시스템에 대한 간략화된 회로를 얻을 수 있다.

[STEP7] 다중 출력인 경우는 각각의 출력에서 구한 결과들의 관계를 조사하여 역시 Ⅳ장에서의 수학적표기 및 각종 유용한 관계를 적용시켜 회로를 구성한다.

위 절차를 흐름도로 나타내면 다음 그림 4-2와 같다.

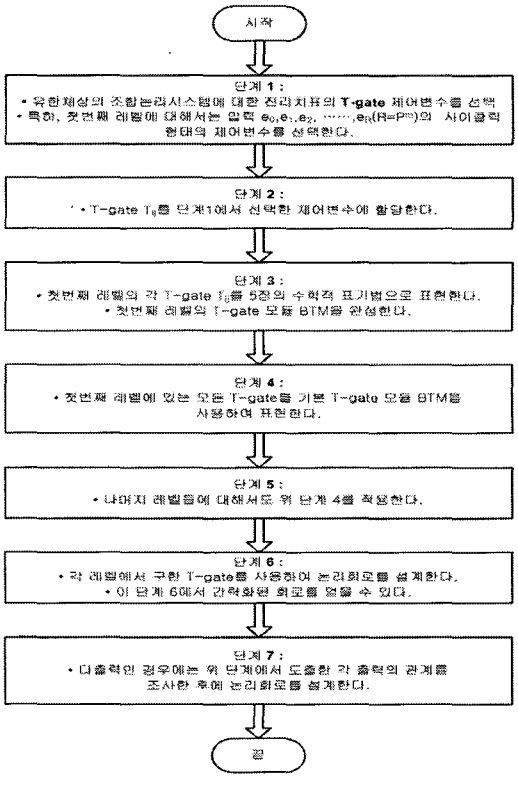


그림 4-2. 유한체상의 디지털논리시스템 구성 절차의 흐름도.
Fig. 4-2. The flow chart of constructing the digital logic systems over Finite Fields.

## VI. 결 론

본 논문에서는 최근에 디지털논리시스템설계시에도 입되고 있는 자동정리증명기법에 기초한 유한체상의 디지털논리시스템 구성의 한가지 방법을 제안하였다. 제안한 개선된 자동정리증명기법의 특징을 요약하면 다음과 같다. 먼저, 유한체의 중요한 수학적 성질을 논의하였으며, Table Pseudo Function Tab과 EQUAL의 개념을 소개하였다. 또한, Building Block으로서 T-gate의 개념과 특징을 논의하였으며, 이를 바탕으로 항등관계, 정수관계, 중복관계 및 Mod R 사이클릭 관계를 도출하였다. 특히Mod R 사이클릭 관계는 좌측 Mod R 사이클릭 관계, 우측 Mod R 사이클릭 관계 및 이들의 혼합사용관계에 대한 성질을 제안하였다. 또한, Mod R 부정 게이트를 사용하여 좀 더 간단하게 디지털논리시스템을 구성하는 방법을 제시하였다. 한편, 디지털논리시스템에서는 무관항의 조건이 존재하며 이를 해결하기 위한 여러 가지 기존의 방법이 제안되고 있다. 본 논문에서는 이들 무관항의 조건을 본 논문에서 제안한 개선된 자동정리증명기법을 이용하여 효과적으로 디지털논리시스템을 구성할 수 있는 한가지 방법을 제안하였다. 제안한 개선된 자동정리증명기법은 기존의 방법에 비해 다양한 관계를 적용시킬 수 가 있었으며 그 결과 기존의 방법에 비해 좀 더 효과적이고 규칙적으로 디지털논리시스템을 구성시킬 수 가 있었다. 향 후 연구과제로는 좀 더 일반화된 자동정리증명기법에 대한 알고리즘의 연구가 요구되며, 이를 바탕으로 디지털논리시스템의 또 다른 한 분야인 순차논리시스템의 구성에 적용하는 연구가 요구된다.

## 참고문헌


[1] W.C.Kabat and A.S.Wojcik,"Automated Synthesis of Combinational Logic using Theorem Proving Techniques," IEEE Proc. 12th ISMVL, pp.178-199, May. 1982.

[2] W.C.Kabat,"Automated Design of Combinational Networks under Specific Constraints: A Theorem Proving Approach," IEEE Proc. 13th ISMVL, pp.366-396, May. 1983.

[3] W.C.Kabat and A.S.Wojcik,"Automated Synthesis of Combinational Logic using Theorem-Proving Techniques," IEEE Trans. Comput., vol.C-34, no.7, pp.610-632, Jul. 1985.

[4] V.J.Sanchez and W.C.Kabat,"Automated Synthesis of Algorithmic State machines," IEEE Proc. 16th ISMVL, pp.265-272, May. 1986.

[5] D.Snyers and A.Thayse,"Algorithmic State Machines Design and Automatic Theorem Proving: Two Dual Approach to the Same Activity," IEEE Trans. Comput., vol.C-35, no.10, pp. 853-861, Oct. 1986.

[6] V.S.Stokkermans,"Representation Theorems and Theorem Proving in Non-Classical Logics," IEEE Proc. 29th ISMVL, pp.242-247, May 1999.

[7] V.S.Stokkermans,"Representation Theorems and the Semantics of (Semi)Lattics-based Logics," IEEE Proc. 31th ISMVL, pp.125-135, May 2001.

[8] H.Ganzinger and V.S.-Stokkermans,"Chaining Techniques for Automated Theorem Proving in Many-Valued Logic," IEEE Proc. 30th ISMVL, pp.337-344, May 2000.


## 저자소개


**박춘명(Chun-MyoungPark)**

1994년 2월 인하대학교 대학원 전자공학과(공학박사)
1995년 9월 ~ 2005년 현재 충주대학교 전기 · 전자 및 정보공학부 컴퓨터공학과 교수

1984년 ~ 2005년 현재 IEEE Computer Society Member
1984년 ~ 2005년 현재 대한전자공학회 정회원
2005년 현재 한국해양정보통신학회 학회지편집위원
2002년 ~ 2003년 UCI(University of California, Irvine) ICS 와 CECS(Center for Embedded Computer Systems) Visiting Scholar

※ 관심분야 : 차세대 디지털논리시스템 및 컴퓨터 구조, 임베디드시스템, 마이크로프로세서 응용, 유비쿼터스컴퓨팅시스템, 멀티미디어시스템 등