연구실 소개

부호 및 정보이론 연구실

지도교수: 송홍엽

박사과정 2명, 석사과정 8명

본 연구실의 연구관심분야는 크게 (1) 부호이론 관련 응용수학 분야 (2) Sequences with Optimal Correlation 분야로 요약된다. 아래에는 이와 관련된 세부적인 내용과 연구과제를 중심으로 자세히 설명하기로 한다. 중심적인 개념은 통신/저장 시스템의 기본 블록을 수학적으로 모델링하고 최적의 성능을 가능케 하는 신호의 모양을 찾아내는 작업이라 정의할 수 있다.

(1) 부호이론 관련 응용수학 분야

기본적으로 디지털 무선통신시스템의 성능향상을 위한 오류정정부호와 관련된 분야이다. 이 분야의 주된 관심은 길이 n과 오류정정능력 t, 그리고 부호어의 수 M이 정해지면 이를 만족하는 부호어의 집합이 존재하는가에 대한 수학적 분야이다. 이러한 부호집합의 대표적인 예는 Hamming 부호, BCH 부호, Reed-Solomon 부호 등이 있다. 이들은 현재 부호화/복호화기 등이 반도체기술의 진보에 따라 상용화되어 있으나, 이론적으로 해결해야할 많은 미완의 문제들이 존재하는데, 그 대표적인 문제는 부호어의 무게분포(Weight Distribution)이다. 위에 열거한 잘 알려진 부호를 제외하고 많은 수의 부호는 아직 무게분포가 완전히 알려져 있지 않은데, 이는 부호의 오류정정 능력과 복호화기의 효과적인 알고리듬 개발을 위해서도 필수적이다. 복호 알고리듬은 통신시스템 뿐만 아니라, 요즈음 각광받는 디지털 저장시스템의 상용화를 위한 중요한 문제로서 깊이 있는 연구가 진행중이다. 이와 관련하여 본 연구실에서는 현재 과학재단 특정기초연구과제를 2년차 수행하고 있다. 본 연구에서는 직교부호 집합을 구성하는 하다마드 행렬과 관련된 오랜 Open Problems에 대한 끊임없는 도전으로 IEEE Transactions on Information Theory와 다양한 국외 수학전문잡지 등에 논문을 발표하고 있다. 그밖에도, 부호이론과 관련된 암호학의 근본적인 수학적 문제, 즉, 인증 및 서명문제, 소수판정법, 소인수분해알고리듬 등에도 관심을 가진다.

(2) Sequences with Optimal Correlation

Spread Spectrum Communication System의 기본을 이루는 Pseudo Noise Sequences에 관련된 이론분야이다. 이진 수열의 랜덤특성을 수학적으로 정의하고 이를 만족하는 최적의 이진수열을 어떻게 구성하며 쉽게 발생시켜 응용할 수 있는가에 대한 연구이다. 대표적으로 1차원 이진수열에는 LFSR Sequences, Gold Sequences, Kasami Sequences 등이 있으며, 최근의 연구결과로 얻어진 최적상관함수를 갖는 많은 이진수열이 새로이 알려졌다. 이는 앞면과 뒷면이 나올 확률이 각각 1/2 인 완전한 동전을 던지는 시행을 연속적으로 수행하여 얻어지는 진정한 의미의 랜덤 시퀀스(Random Sequence)의 특성을 충실히 갖추면서도 그 발생 과정은 결정적(Deterministic)이기 때문에 다음과 같은 다양한 분야에 이용되고 있다.

- ▣ IS95 CDMA 이동 통신의 물리계층
- ▣ Spread-Spectrum 통신 시스템
- ▣ Geostationary Positioning Satellite 신호
- ▣ 레이더 및 디지털 통신의 동기 신호
- ▣ Exclusive-OR를 사용하는 암호시스템
- ▣ 반도체 집적회로 등의 시험 및 계측 시스템
- ▣ 부호이론
- ▣ Statistical Design of Experiments

또한, 2차원 신호에는 Radar Array Code, Sonar Array Code 등이 있고, 이들의 목적은 주어진 환경에서 2차원 Correlation특성이 최적으로 모델링된 신호로서 통신/레이더/소나 시스템의 거리/속도/영상 측정의 resolution을 극대화시키자는 것이다. 이와 관련하여 역시 IEEE Transactions on Information Theory 등에 많은 논문을 발표하고 있으며, 현재 정보통신부 대학기초과제로 3년차를 마치는 중이며, 연속적으로 제안서를 제출, 심사 중에 있다.

(3) 기타 준비중에 있는 연구과제

암호기술관련 분야와 Turbo Code의 복호화기 성능분석, 그리고 Frequency-Hopping Spread Spectrum 통신 시스템 과 IS95-based CDMA 통신 시스템의 성능분석에 관한 연구과제를 준비중에 있다. 향후, 부호이론/정보이론 분야의 국내 연구기반의 한 축을 담당할 것으로 생각된다.