

심볼 단위 길쌘 인터리버의 파라미터 추정

박세훈, 장연수, 윤동원
한양대학교

Parameter Estimation of Symbol Unit Convolutional Interleaver

Sehoon Park · Yeonsoo Jang · Dongweon Yoon

Hanyang University

E-mail: dwyoon@hanyang.ac.kr

요 약

디지털 통신 시스템에서 인터리버는 채널상에서 발생하는 연접 오류를 분산시켜 랜덤한 오류로 바꾸어 준다. 그 결과로 신호는 특정 방식으로 재배치되고 송신단의 정보를 모르는 제 3자에 대해서 이 신호는 암호화 된다. 이러한 미지의 신호를 복원해 내는 기술은 전자전에 있어서 매우 중요하며 이에 대한 기존의 연구는 주로 비트단위 인터리버나 헬리컬 스캔 인터리버 추정에 대해 이루어져 왔다. 본 논문에서는 채널 부호의 선형성을 이용하여 단축 리드 솔로몬 부호화된 신호의 심볼 단위 길쌘 인터리버 단 수, 부호어 길이, 부호어 정보 심볼 수 등의 인터리버 파라미터를 추정하는 알고리즘을 제안한다. 그리고 컴퓨터 모의실험을 통해 이를 검증한다.

ABSTRACT

In digital communications systems, an interleaver spreads burst errors occurred in channels and makes it random errors. As a result, the signals are rearranged and encrypted to the 3rd party. Deinterleaving this unknown interleaved signal is very important in electronic warfare and various researches on reconstruction of interleaved signal have been studied in the literature. Unlike previous researches which is mainly about helical scan interleaver or bit unit interleaver, in this paper, we estimate the symbol unit convolutional interleaver and shortened Reed-Solomon code parameters such as the number of stages of interleaver, a codeword length and a data symbol length and propose an specific algorithm to obtain the parameters from the unknown interleaved signal and simulate this algorithm as well.

키워드

convolutional interleaver, interleaver parameter, shortened Reed-Solomon code, communications systems

I. 서 론

디지털 통신에서 채널 부호화는 신호가 채널을 통과할 때 생기는 신호의 왜곡에 대해서 수신기가 원신호를 신뢰성 있게 복원할 수 있도록 하기 위해 사용된다[1]. 이 논문에서 중점적으로 다루게 될 리드 솔로몬 부호는 리드와 솔로몬이 제안한 비이진 BCH(Bose, Chaudhri, and Hocquenghem)부호의 하나이다[2]. 리드 솔로몬 부호는 심볼 단위로 부호화되고 복호되기 때문에 채널 상에서 발생하는 산발오류와 연접오류를 모두 정정할 수 있어 각종 디지털 통신 시스템 및 데이터 저장 시스템의 신뢰성 향상 대책으로 광범위하게 사용되고 있다. 또한 이 부호는 정보 심볼과 정보 심볼의 선형 조합의 결과인 잉여 심볼로 구성되는데 정보 심볼 중 필요 없는 상위 심볼은 모두 영으로 하여 단축된 리드 솔로몬 부호

로도 사용될 수 있다[2].

리드 솔로몬 부호와 더불어 인터리빙은 통신 시스템의 신뢰성을 높여준다. 인터리버는 채널 부호화된 정보를 분산시켜 채널 환경에서 발생하는 연접오류를 랜덤 비트 오류로 바꿀 수 있으며, 이는 통신 성능과 신뢰성을 향상시켜 줄 뿐만 아니라 이에 대한 정보가 없는 제 3자에 대해 암호화 역할을 수행할 수 있게 만든다[2],[3].

기존 연구는 송신단에 대한 정보가 없을 때 비트단위 길쌘 인터리버 또는 헬리컬 스캔 인터리버의 파라미터를 추정하는데 초점을 맞춰 왔다. 이러한 기존 연구와 달리 이 논문은 심볼 단위 길쌘 인터리버의 파라미터 추정 알고리즘과 그에 따른 신호 복원에 대한 연구를 다룬다.

본 논문의 구성은 다음과 같다. 2장에선 심볼 단위로 길쌘 인터리빙 된 리드 솔로몬 부호를 길쌘 인터리버의 매개 변수를 추정하여 디인터리빙

하는 알고리즘을 제안하고 3장에선 모의실험결과를 제시하며, 마지막 4장에선 논문에 대한 결론을 맺는다.

II. 인터리버 파라미터 추정

1. 심볼 단위 길쌘 인터리빙 신호의 특징

송신되는 신호의 특징을 살펴보기 위해선 어떤 부호가 어떤 과정을 거쳐 송신되는지 확인해야 한다. 이 과정은 임의의 데이터가 단축 리드 솔로몬 부호(Shortened Reed-Solomon, SRS)로 부호화되는 것부터 시작된다. 임의의 단축 리드 솔로몬 부호는 각 심볼이 m비트인 A개의 심볼로 구성되어 있고 그 중 B개가 정보 심볼인 리드 솔로몬(Reed-Solomon, RS) 부호로부터 생성된다[2]. 리드 솔로몬 부호에 대한 표현을 RS(A, B)라 한다면, 이 부호의 나머지 (A-B)심볼은 오류정정을 위해 사용되고 B개의 정보 심볼의 선형조합을 통해 만들어 진다[3]. 이때 리드 솔로몬 부호의 길이가 전송하고자 하는 정보 심볼의 길이보다 훨씬 더 길다면 상당히 비효율적일 수 있다. 이를 보완하기 위해 리드 솔로몬 부호는 단축 리드 솔로몬 부호로 변환된다. 단축 리드 솔로몬 부호는 비효율적으로 긴 심볼의 길이를 줄이기 위해서 사용되는 방식으로, 실제로 사용되는 정보 심볼의 수를 제외한 나머지 상위 1개의 정보 심볼을 모두 0으로 하여 구한 (A-1, B-1)의 부호로써 n=A-1, k=B-1이라 한다면 SRS(n, k)로 표현될 수 있다[2].

부호화가 끝난 후 단축 리드 솔로몬 부호는 인터리빙 과정을 거치게 된다. 인터리버는 크게 블록 인터리버, 길쌘 인터리버, 랜덤 인터리버로 분류되며, 이 중 이 논문에서 다루게 될 길쌘 인터리버가 심볼 단위로 데이터를 재배치하는 방식을 그림 1에 나타내었다. 그림 1은 3단짜리 길쌘 인터리버의 입/출력 예를 보여준다. 숫자 C1, C2, C3은 각각 첫 번째, 두 번째, 세 번째 심볼을 의미하며 오른쪽 사각형은 쉬프트 레지스터 역할을 하게 되어 첫 번째 단 두 번째 단 세 번째 단은 각각 한번 두 번 세 번의 딜레이를 거치게 된다.

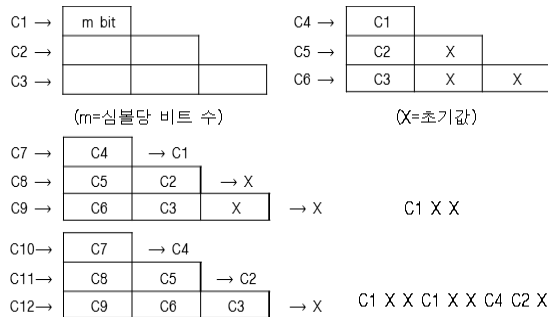


그림 1. 길쌘 인터리버의 입/출력

인터리빙을 n열의 행렬로 살펴보면, 조금 더 쉽게 n단짜리 길쌘 인터리빙의 규칙성을 찾을 수 있다[3],[4]. 실제로 하나의 심볼이 m비트이기 때문에 n열이 아닌 n×m열 이지만 여기선 각 열을 심볼 단위로 바꾸어 n열로 표현한다. 그림2는 단축 리드 솔로몬 부호가 3단짜리 길쌘 인터리버에 의해 재배치되는 과정을 3열의 행렬로 보여주고 있다. n단짜리 인터리버의 출력을 n열의 행렬로 나타내면, 심볼이 행렬의 대각선 방향을 따라 순차적으로 위치하고 있다는 것을 확인할 수 있다. 즉, 단축 리드 솔로몬 부호 SRS(n,k) s개를 n단짜리 길쌘 인터리버의 입력으로 넣을 때 인터리빙되는 순서는 다음과 같다. 먼저 s개의 부호를 각각 n열의 행렬의 행으로 표현하고 q번째 열을 q-1행 쉬프트 한다. 이때 비어있는 부분을 초기값 X로 채우면 (s+n-1)×n 크기의 행렬로 표현되고 인터리버의 출력은 이 행렬을 행 순서대로 배열한 값이라 할 수 있다.

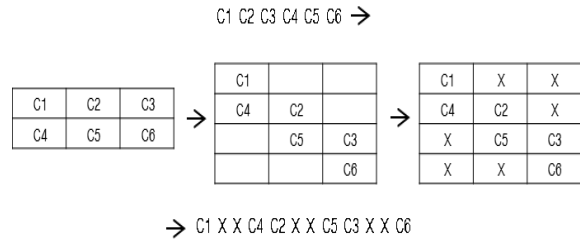


그림 2. 3열의 행렬로 표현한 3단 길쌘 인터리빙

2. 선형성을 이용한 파라미터 추정 및 디인터리빙

이 장에서는 송신단에서 어떤 리드 솔로몬 부호를 사용했고 인터리버 파라미터를 사용했는지 알 수 없을 때, 이에 대해서 추정하고 디인터리빙하는 방식에 대해서 설명한다. 수신단에서 받은 신호를 디인터리빙을 하기 위해선 가장 먼저 몇 단짜리 길쌘 인터리버가 사용되었는지 알아야 한다. 이를 위해 신호가 올바르게 디인터리빙 되었을 때와 그렇지 못할 때를 비교해 봐야할 필요가 있다. 디인터리빙 방식은 인터리빙 방법의 역순이 된다. 즉, 신호가 n단 길쌘 인터리빙된 신호라고 추정된다면 n열의 행렬로 신호를 채워 넣은 뒤 두 번째 열은 1행 위로 쉬프트 세 번째 열은 2행 위로 쉬프트 q번째 열은 q행 위로 쉬프트 하여 디인터리빙 할 수 있다. 그림3은 3단 길쌘 인터리버에 의해 생성된 신호가 올바르게 디인터리빙 되었을 경우의 행렬 모습과 그렇지 못할 때의 행렬 모습을 보여준다. 올바르게 디인터리빙 되었을 경우엔 각 행이 독립된 1개의 단축 리드 솔로몬 부호가 되는 반면에 그렇지 못한 경우엔 1개의 단축 리드 솔로몬 부호가 여러 행으로 나누어진 다.

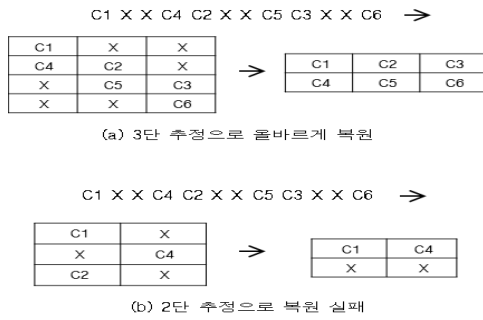


그림 3. 3단 길쌈 인터리빙된 신호의 디인터리빙

각 행이 단축 리드 솔로몬 부호 단위로 구성되어 있음을 확인하는 방법은 다음과 같다. 디인터리빙된 행렬의 전치 행렬을 생각해 볼 때, 올바르게 디인터리빙된 행렬은 단축 리드 솔로몬 부호가 열로 세워져 있는 모습이며 가우스 소거시에 각 행의 선형조합을 통해 잉여 심볼들로 구성된 행을 제거할 수 있다. 이 행렬의 행계수(row rank)는 심볼당비트수(m)×정보심볼수(k)가 될 것이다[5]. 반면에 잘못 디인터리빙된 경우엔 정보 심볼과 잉여 심볼이 서로 다른 행으로 어긋나 있기 때문에 가우스 소거시 거의 모든 행이 독립적일 것이다. 위와 같은 기본 이론을 바탕으로 한 알고리즘은 아래와 같다.

- 1) 만약 부호가 각 심볼이 m 비트로 구성된 n 단 인터리버를 통해 인터리빙 된 SRS(n, k) 라면 한 개의 부호는 $m*n$ 비트로 구성되어 있을 것이다. 이때 신뢰성 있는 결과 도출을 위해 $2*m*n$ 개의 부호를 추출한다. 즉, $(2*m*n+n-1)*(n*m)$ 비트를 수신된 신호로부터 추출하여 $(2*m*n+n-1) \times (n*m)$ 의 행렬을 만든다.
- 2) 추출된 행렬을 통해 디인터리빙한다. 이때 인터리버의 초기값 X 는 0으로 가정한다.
- 3) 디인터리빙된 행렬의 전치행렬을 가우스 소거한다.
- 4) $m*n+1$ 열부터 $2*m*n$ 열까지의 각 행의 0에 대한 1의 비율 R 을 측정한다.
- 5) 인터리버 단수 n 을 예상되는 추정범위 내의 값으로 바꿔가며 1)~4) 과정을 반복한다.
- 6) R 값이 특정 행부터 계속 0으로 유지될 때 인터리버의 단수를 구한다.
- 7) 이때 (비율이 갑자기 0으로 되기 시작한 행 - 1)/ m 값이 단축 리드 솔로몬 부호의 정보 심볼 개수가 된다.

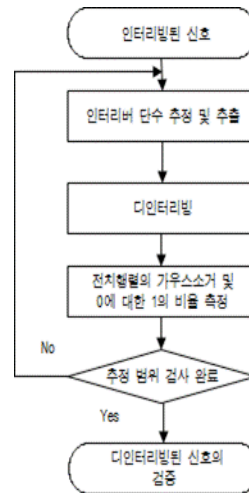


그림 4. 신호의 디인터리빙 및 인터리버 파라미터 추정 알고리즘

III. 모의실험 결과

이 장에서는 위에서 제시된 이론을 바탕으로 한 모의실험 결과를 나타내었다. 모의실험의 순서와 방법은 다음과 같다.

- 1) 심볼당 비트수 $m=5$ 비트인 SRS(27,3)을 발생시키고 이를 심볼단위로 길쌈 인터리빙하여 송신단의 신호를 만든다.
- 2) 제시된 알고리즘을 통해 주어진 신호의 파라미터를 추정한다. 이때 인터리버 단수의 추정범위는 $25 \leq n \leq 30$ 이며, 각 행의 0에 대한 1의 비율 $R=(\text{각 행의 1의 개수})/(\text{각 행의 0의 개수})$ 로 표현한다.

위의 실험결과를 그림5와 6을 통해 확인할 수 있다.

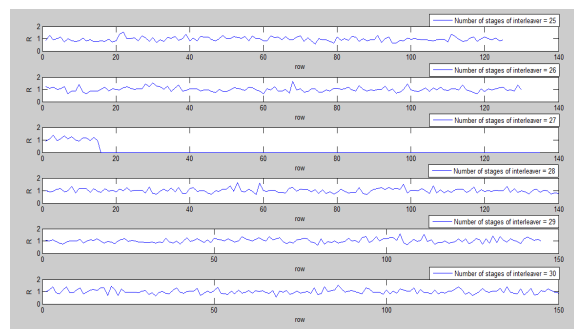


그림 5. 가우스 소거 후 각 행의 0에 대한 1의 비율 (위쪽부터 차례대로 25/26/27/28/29/30)

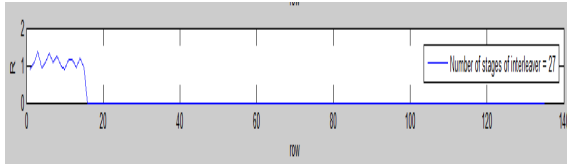


그림 6. 인터리버 단수가 27일 때 R=0이 된 지점

그림5와 6을 통해 올바르게 디인터리빙 된 신호가 어떻게 가우스 소거 되는지 알 수 있다. 올바르게 디인터리빙 된 신호는 가우스 소거시에 잉여 심볼을 전부 소거하게 되어 정보 심볼 수를 제외한 심볼은 전부 0으로 나타난다. 반면에 올바르게 디인터리빙 되지 않았을 경우 각 행은 독립성을 유지하며 각 행의 0과 1의 비율이 거의 같게 나타남을 확인할 수 있다. 즉 이 신호는 27단 길쌈 인터리버로 인터리빙 되었음을 알 수 있고 16번째 행에서 0으로 떨어졌기 때문에 단축 리드 솔로몬 부호의 정보 심볼 길이가 $15/m=3$ 임을 확인할 수 있다.

IV. 결 론

이 논문에서는 미지의 송신단에서 구성된 단축 리드 솔로몬 부호와 길쌈 인터리버의 파라미터를 추정하여 원래 신호를 복원하는 방법과 그에 대한 구체적인 알고리즘을 제시하였다. 또한 제시한 알고리즘을 통해 모의실험을 시행하였고 올바르게 적용됨을 확인하였다. 이 결과는 미지의 통신 시스템에서 구성된 신호를 디인터리빙하는 기본 알고리즘을 제공하며, 향후 다양한 채널환경과 잡음을 고려한 효율적인 디인터리빙에 대한 연구에 적용 가능할 것으로 기대된다.

참고문헌

- [1] B. Sklar, Digital Communications: Fundamentals and Applications, Prentice-Hall International, Inc., 2001.
- [2] 이만영, BCH 부호와 Reed-Solomon 부호, 민음사, 1990.
- [3] 이주병, 정정훈, 김상구, 김탁규, 윤동원, “채널 부호의 선형성을 이용한 길쌈 인터리버의 파라미터 추정”, 전자공학회 논문지, 제 48권 TC편 제 4호, pp.15-23, 2011년 4월.
- [4] 이주병, 정정훈, 윤동원, 윤상범, 박영미, 나선필, “헬리컬 스캔 인터리버 파라미터 추정 및 복원”, 국방과학연구소 창설 40주년 기념 종합학술대회, pp.360-362, 2010년 8월.
- [5] G. Strang, Linear Algebra and Its Applications(4th ed.), Thomson Learning Inc., 2006.