김일성종합대학학보
(자연과학)
주체105(2016)년 제62권 제2호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 62 No. 2 JUCHE105(2016).

백색가우스잡음통로우에서 저밀도기우성검사부호의 변형된 합－적복호오유수정모임을 결정하는 계산의 복잡성

송정윤, 김철은

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《현시대는 과학과 기술의 시대이며 과학과 기술이 류례없이 빠른 속도로 발전하는것은 현대과학기술발전의 중요한 특징입니다.》(《**김정일**선집》 증보판 제15권 485페지)

론문에서는 최근 부호화리론에서 비약적으로 발전하고있는 저밀도기우성검사부호(LDPC부호)의 복호법에 대하여 론의하였다.

선행연구[1]에서는 LDPC부호를 정의하고 이 부호가 합－적복호를 진행할 때 쉐논(Shannon)한계에 도달하는 부호라는것을 밝혔으며 선행연구[2]에서는 2원대칭통로(BSC)우에서 LDPC부호의 합－적복호법을 변형하고 오유수정모임에 대한 리론적평가를 주었다.

우리는 선행연구[2]의 결과를 백색가우스잡음통로우에로 확장하여 오유수정모임과 신드롬모임사이의 관계를 설정하여 오유수정모임을 결정하는 계산복잡도를 줄이였으며 기우성검사행렬의 대칭성을 리용하여서도 계산복잡성을 줄이였다.

1. 변형된 합－적복호기와 오유수정모임

다음과 같은 통신모형을 생각하자.

송신자는 검사행렬 H 를 가진 2진LDPC부호의 부호단어 c 를 선택하고 가법적백색잡음통로로 전송한다.

통로의 출력모임과 오유확률을 리산화한다.

구간 $(-\infty, +\infty)$ 를 $2L+2$ 개 구간으로 분할하고 오유확률을 표와 같이 정의한다.

표에서 $q_1 = \int_0^1 \Phi(x+a)dx \Big/ \left(\int_0^1 \Phi(x+a)dx + \int_0^1 \Phi(x-a)dx \right)$,

$q_2 = \int_1^2 \Phi(x+a)dx \Big/ \left(\int_1^2 \Phi(x+a)dx + \int_1^2 \Phi(x-a)dx \right)$, $\cdots$,

$q_{L+1} = \int_L^\infty \Phi(x+a)dx \Big/ \left(\int_L^\infty \Phi(x+a)dx + \int_L^\infty \Phi(x-a)dx \right)$,

$$\Phi(x) = \frac{1}{\sqrt{2\pi}\sigma} \cdot e^{-x^2/(2\sigma^2)}.$$

표. 구간분할에 따르는 오유확률

구간	리산화	0	1
$(-\infty, -L)$	$-L$	$1-q_{L+1}$	q_{L+1}
$(-L, -L+1)$	$-L+1$	$1-q_L$	q_L
⋮	⋮	⋮	⋮
$(-1, 0)$	0	$1-q_1$	q_1
$(0, 1)$	1	q_1	$1-q_1$
$(1, 2)$	2	q_2	$1-q_2$
⋮	⋮	⋮	⋮
$(L, +\infty)$	$L+1$	q_{L+1}	$1-q_{L+1}$

수신자는 파라메터 H, $l_{\max}$, q 와 수신된 단어 r 를 합적복호기(SPDec)에 입력한다. 여기서 $l_{\max}$ 는 최대반복수라고 부르는 파라메터이다.

출력값이 c 이면 통신은 성공하며 그렇지 않다면 실패한다. 단어오유률은 통신의 실패확률이다.

론문에서는 가법적백색잡음통로우에서의 합－적복호기를 리용한 LDPC부호의 단어오유률을 해석한다.

우리는 먼저 합－적복호알고리듬을 변형한다.

s를 신드롬이라고 부르는 어떤 렬, $H=(H_{m,\,n})$을 $M\times N$인 2진행렬이라고 하자.

$A(m)$, $B(n)$, E를 다음과 같이 정의한다.

$A(m)=\{1\le m\le M \mid H_{m,\,n}=1\}$, $B(m)=\{1\le n\le N \mid H_{m,\,n}=1\}$, $E=\{\pm 0,\ \pm 1,\ \cdots,\ \pm 2L+1\}$

변형된 합－적복호알고리듬은 다음과 같다.

입력: 기우성검사행렬 $H=(H_{m,\,n})_{M\times N}$, 수신신호렬 $r=(r_1,\ r_2,\cdots,\ r_N)^{\mathrm{T}}$, 오유확률벡토르 $p=(p_1,\ p_2,\cdots,\ p_{L+1})^{\mathrm{T}}$, 최대반복수 $l_{\max}$, 신드롬 $s=(s_1,\ s_2,\cdots,\ s_M)^{\mathrm{T}}\in\{0,\ 1\}^M$

출력: $c=(c_1,\ c_2,\cdots,\ c_N)^{\mathrm{T}}\in\{0,\ 1\}^N$

단계 1(초기화) $H(m,\ n)=1$인 모든 $(m,\ n)$과 $x\in E$에 대하여 $q_{m,\,n}(x)=\dfrac{1}{2}$로 초기화한 다음 $z=(z_1,\ z_2,\cdots,\ z_M)=rH^{\mathrm{T}}$를 계산한다.

단계 2(행처리) $\forall m(1\le m\le M),\ n\in A(m),\ x\in E$

$$r_{m,\,n}(x)=K_{m,\,n}\sum_{\left\{\{x_{n'},\ n'\in A(m)\backslash\{n\}:x\oplus z_n\oplus s_n\oplus a\mid A(m)\mid=\sum_l x_l\right\}}\ \prod_{l\in A(m)\backslash\{n\}}q_{m,\,l}(x_l)p(r_l\mid x_l)$$

여기서 $r\ge 0$일 때 $p(r\mid x)=\begin{cases}p_r, & r-x=-a\\ 1-p_r, & r-x=a\\ 0, & r-x\ne\pm a\end{cases}$, $r<0$일 때 $p(r\mid x)=\begin{cases}p_{-r+1}, & r-x=a\\ 1-p_{-r+1}, & r-x=-a\\ 0, & r-x\ne\pm a\end{cases}$이며 $K_{m,\,n}$은 $\sum\limits_x r_{m,\,n}(x)=1$인 상수이다.

단계 3(렬처리) $\forall n\ (1\le n\le N),\ m\in B(n),\ x\in E,\ q_{m,\,n}(x)=K'_{m,\,n}\prod\limits_{l\in B(n)\backslash\{m\}}r_{l,\,m}(x)$

여기서 $K'_{m,\,n}$은 $\sum\limits_x q_{m,\,n}(x)=1$인 상수이다.

단계 4(림시오유결정) $\forall n\ (1\le n\le N),\ x\in E,\ q_n(x)=K''_{m,\,n}q(r_n\mid x_n=x)\prod\limits_{l\in B(n)}r_{l,\,m}(x)$

다음 $\hat{c}_n=\arg\max\limits_x q_n(x)$를 결정한다. 여기서 $K''_{m,\,n}$은 $\sum\limits_x q_n(x)=1$인 상수이다.

단계 5(기우성검사) $(\hat{c}_1,\ \hat{c}_2,\cdots,\ \hat{c}_N)H^{\mathrm{T}}=s^{\mathrm{T}}$이면 매 i에 대하여 $c_i=\dfrac{(r_i-\hat{c}_i)/a+1}{2}$을 계산한 다음 $(c_1,\ c_2,\cdots,\ c_N)$을 출력한다.

단계 6(반복의 련속) $l<l_{\max}$이면 단계 2로, $l=l_{\max}$이면 출력은 실패를 선언한다.

정의 1 $\mathrm{SPDec}[H,\ 0+r,\ p,\ l_{\max}]=0$인 r들의 모임을 오유수정모임이라고 하며 $\varepsilon_{H,\ p,\ l_{\max}}$로 표시한다. 즉

$$\varepsilon_{H,\ p,\ l_{\max}}=\{r\mid \mathrm{SPDec}[H,\ 0+r,\ p,\ l_{\max}]=0\}.$$

2. 신드롬복호와 오유수정모임

여기서는 신드롬복호($s \neq 0$일 때 합－적복호를 신드롬복호라고 부른다.)와 오유수정모임과의 관계를 론의한다.

우리는 합－적신드롬복호기의 출력을 SynDec$[H,\ r,\ p,\ l_{\max},\ s]$로 표시한다.

정리 1 임의의 $H,\ r,\ p,\ l_{\max}$에 대하여 다음의 결과들은 동등하다.

$$\mathrm{SPDec}[H,\ 0+r,\ p,\ l_{\max}]=0,\ \ \mathrm{SynDec}[H,\ 0,\ p,\ l_{\max},\ Hr^{\mathrm{T}}]=0$$

보조정리 $Q,\ R$를 SPDec$[H,\ 0+r,\ p,\ l_{\max}]$, $\overline{Q},\ \overline{R}$를 SynDec$[H,\ 0,\ p,\ l_{\max},\ Hr^{\mathrm{T}}]$에 대응하는 행렬들이라고 하면 임의의 $m\ (1\le m\le M)$, $n\ (1\le n\le N)$, $l\ (1\le l\le l_{\max})$, $x\in E$에 대하여 다음의 결과들이 성립된다.

$$q_{m,\,n}(x)=\overline{q}_{m,\,n}(x-r_n),\ \ r_{m,\,n}(x)=r_{m,\,n}(x-r_n),\ \ q_n(x)=\overline{q}_n(x-r_n)$$

증명 SPDec와 SynDec복호기를 동시에 관측하면 귀납적으로 쉽게 증명할수 있다.

단계 1 $A(m,\ n)=1$인 모든 $(m,\ n)$에 대하여 $q_{m,\,n}(x)=\overline{q}_{m,\,n}(x-r_n)=1/2$이며 임의의 n에 대하여 $z_n=\overline{s}_n$이 성립된다. 복호의 l째 반복에서 보조정리가 성립된다고 하고 $(l+1)$째 반복에서 성립된다는것을 증명한다.

단계 2(행처리) $\forall m,\ n\in A(m),\ x\in E$

$$r_{m,\,n}(x)=K_{m,\,n}\sum_{\left\{x_{n'},\ n'\in A(m)\setminus\{n\}:x\oplus z_n\oplus a|A(m)|=\sum_l x_l\right\}}\ \prod_{l\in A(m)\setminus\{n\}}q_{m,\,l}(x_l)\,p(r_l\mid x_l)=$$

$$=K_{m,\,n}\sum_{\left\{x_{n'},\ n'\in A(m)\setminus\{n\}:(x-r_n)\oplus s_n\oplus a|A(m)|=\sum_l(x_l-r_l)\right\}}\ \prod_{l\in A(m)\setminus\{n\}}\overline{q}_{m,\,l}(x_l-r_l)\,p(0\mid x_l-r_l)=\overline{r}_{m,\,n}(x-r_n)$$

단계 3(렬처리)

$$\forall n,\ m\in B(n),\ x\in E,\ q_{m,\,n}(x)=K'_{m,\,n}\prod_{l\in B(n)\setminus\{m\}}r_{l,\,m}(x)=K'_{m,\,n}\prod_{l\in B(n)\setminus\{m\}}\overline{r}_{l,\,m}(x-r_n)=\overline{q}_{m,\,n}(x-r_n)$$

단계 4

$$\forall n,\ x\in E,\ q_n(x)=K''_{m,\,n}q(r_n\mid x_n=x)\prod_{l\in B(n)}r_{l,\,m}(x)=K''_{m,\,n}q(0\mid x_n=x-r_n)\prod_{l\in B(n)}\overline{r}_{l,\,m}(x-r_n)=\overline{q}_n(x-r_n)$$

(증명끝)

정리 1의 증명 복호의 l_0반복에서 SPDec$[H,\ 0+r,\ p,\ l_{\max}]=0$이기 위한 필요충분조건으로부터 임의의 l반복에서 기우성검사가 만족되지 않는다. l_0반복에서 모든 n에 대하여 $q_n(r_n)=\max\limits_x q_n(x)$가 성립되고 이로부터 임의의 l반복에서 기우성검사가 만족되지 않으며 l_0반복에서 모든 n에 대하여 $q_n(r_n-r_n)=\max\limits_x q_n(x-r_n)$이 성립된다.

따라서 복호의 l_0반복에서 SynDec$[H,\ 0,\ p,\ l_{\max},\ Hr^{\mathrm{T}}]=0$이 성립된다.(증명끝)

정리 2 주어진 $H,\ p,\ l_{\max}$에 대하여 다음의 결과가 성립된다.

$$\varepsilon_{H,\ p,\ l_{\max}}=\{r\mid\mathrm{SynDec}[H,\ 0,\ p,\ l_{\max},\ s]=0,\ Hr^{\mathrm{T}}=s\}$$

우리는 SynDec$[H,\ 0,\ p,\ l_{\max},\ s]=0$을 만족시키는 s를 복호가능한 신드롬이라고 정의하고 복호가능한 신드롬들의 모임을 $D_{H,\ p,\ l_{\max}}$로 표시한다.

3. 그라프동형과 오유수정모임

H가 $M\times N$ 형저밀도기우성검사행렬이고 σ가 첨수모임 $[M]=\{1, 2, 3, \cdots, M\}$우의 치환이라고 하면 치환 σ는 자연스럽게 H의 렬에 작용한다.

σH를 σ에 의한 H의 치환된 행렬, σs를 렬벡토르 s의 치환된 벡토르라고 한다.

류사하게 τ를 첨수모임 $[N]=\{1, 2, \cdots, N\}$우에서의 치환이라고 하고 $H\tau$, $s\tau$를 각각 행렬 H와 행벡토르 s의 치환된 결과라고 하자.

정리 3 H, p, $l_{\max}$가 주어졌다고 하면 임의의 렬 r에 대하여 다음의 결과들은 동등하다.

i) $\mathrm{SPDec}[H,\ 0+r,\ p,\ l_{\max}]=0$

ii) $\mathrm{SPDec}[\sigma H,\ 0+r,\ p,\ l_{\max}]=0$

iii) $\mathrm{SPDec}[H\tau,\ 0+r\tau,\ p,\ l_{\max}]=0$

여기서 σ는 H의 행첨수모임우에서의 치환, τ는 H의 렬첨수우에서의 치환이다.

증명 결과 i), ii)의 동등성은 합－적복호기의 정의로부터 나온다.

왜냐하면 임의의 행치환은 단계 4에서의 림시오유결정을 변화시키지 못하기때문이다.

다음의 식에 의하여 결과 i), iii)의 동등성은 분명하다.

$$\mathrm{SPDec}[H\tau,\ 0+r\tau,\ p,\ l_{\max}]=\mathrm{SPDec}[H,\ 0+r,\ p,\ l_{\max}]\tau$$

이것은 합－적복호의 정의로부터 나오는것이다.(증명끝)

정리 4 H, p, $l_{\max}$가 주어졌다고 하면 임의의 r에 대하여 다음의 결과들은 동등하다.

i) $\mathrm{SynDec}[H,\ 0,\ p,\ l_{\max},\ r^{\mathrm{T}}H]=0$

ii) $\mathrm{SynDec}[H\tau,\ 0,\ p,\ l_{\max},\ r^{\mathrm{T}}H]=0$

LDPC행렬의 기우성검사행렬 H는 2조그라프 $([M], [N], H)$에 의하여 특성화된다. 여기서 $[M]=\{1, 2, 3, \cdots, M\}$, $[N]=\{1, 2, \cdots, N\}$.

이 2조그라프들을 H의 랜너(Tanner)그라프라고 부른다.

그러므로 LDPC부호의 자기동형을 그것의 Tanner그라프에 의하여 정의하는것은 자연스러운것이다.

정의 2 $\sigma^{-1}H\tau=0$을 만족시키는 치환쌍 (σ, τ)를 기우성검사행렬 H를 가지는 LDPC부호의 자기동형이라고 정의한다.

만일 자기동형들사이의 적을 $(\sigma_1, \tau_1)\times(\sigma_2, \tau_2)=(\sigma_1\sigma_2, \tau_1\tau_2)$로 정의하면 자기동형들은 유한군 $\mathrm{Aut}(H)$를 형성한다.

우리는 σ와 τ를 각각 H의 치환으로 가정한다.

따라서 σ와 τ는 H의 첨수치환으로서 작용한다.

자기동형은 Tanner그라프를 고정시키기때문에 다음의 결과들이 나온다.

정리 5 H를 기우성검사행렬, $\varepsilon_{H,\ p,\ l_{\max}}$를 오유수정모임, $D_{H,\ p,\ l_{\max}}$를 복호가능한 신드롬모임이라고 할 때 다음의 결과들이 성립된다.

i) 임의의 오유벡토르 r와 자기동형 (σ, τ)에 대하여 $r\in\varepsilon_{H,\ p,\ l_{\max}} \Leftrightarrow r\tau\in\varepsilon_{H,\ p,\ l_{\max}}$.

ii) 임의의 신드롬 s와 자기동형 (σ, τ)에 대하여 $s\in D_{H,\ p,\ l_{\max}} \Leftrightarrow \sigma s\in D_{H,\ p,\ l_{\max}}$.

증명 i) 오유수정모임의 정의에 의하여 $r \in \varepsilon_{H,\ p,\ l_{\max}} \Leftrightarrow \mathrm{SPDec}[H,\ 0+r,\ p,\ l_{\max}]=0$ 이며 정리 3에 의하여 $\mathrm{SPDec}[H,\ 0+r,\ p,\ l_{\max}]=0 \Leftrightarrow \mathrm{SPDec}[H\tau,\ 0+r\tau,\ p,\ l_{\max}]=0$ 이다.

$(\sigma,\ \tau)$가 H의 자기동형이므로

$$\mathrm{SPDec}[H\tau,\ 0+r\tau,\ p,\ l_{\max}]=0 \Leftrightarrow \mathrm{SPDec}[\sigma H,\ 0+r\tau,\ p,\ l_{\max}]=0 \Leftrightarrow$$
$$\Leftrightarrow \mathrm{SPDec}[H,\ 0+r\tau,\ p,\ l_{\max}]=0 \Leftrightarrow r\tau \in \varepsilon_{H,\ p,\ l_{\max}}$$

ii) $s \in D_{H,\ p,\ l_{\max}} \Leftrightarrow \mathrm{SynDec}[H,\ 0,\ p,\ l_{\max},\ s]=0$

그러면 적당한 r가 있어서 $s=Hr^{\mathrm{T}}$가 성립되며 정리 4에 의하여 $r\tau \in \varepsilon_{H,\ p,\ l_{\max}}$가 성립된다. 그러므로 $Hr^{\mathrm{T}} \in D_{H,\ p,\ l_{\max}}$가 성립된다.

$(\sigma,\ \tau)$가 H의 자기동형이므로 $(\sigma^{-1},\ \tau^{-1})$도 자기동형이다.

τ가 치환이므로 $\tau^{\mathrm{T}}=\tau^{-1}$이다. 그러므로 $H(r\tau)^{\mathrm{T}}=Hr^{-1}r^{\mathrm{T}}=\sigma Hr^{\mathrm{T}}=\sigma s$이며 따라서 $\sigma s \in D_{H,\ p,\ l_{\max}}$이다.(증명끝)

$L=0$인 경우에 (3, 11)형태의 FSA부호의 오유수정모임을 결정하기 위하여 2^{31}개의 연산을 실시하여야 하는데 우의 정리를 리용하면 $2^{24.1}$개의 연산만 실시하면 된다.

참 고 문 헌

[1] R. G. Gallager; Low Density Parity Check Codes, MA：MIT Press, 23～124, 1963.

[2] M. Hagiwara et al.; IEEE Transactions on Information Theory, 58, 4, 2321, 2012.

주체104(2015)년 10월 5일 원고접수

Computational Complexity for Determining Correctable Error Set of Transformed Sum-Product Decoding in LDPC Codes over a White Gaussian Noise Channel

Song Jong Yun, Kim Chol Un

We research the correctable error set for sum-product decoding of LDPC code.

We suggest the transformed sum-product decoding algorithm of LDPC code over a white Gaussian noise channel and study the method that reduces computational complexity of the correctable error set.

Key word: LDPC code