論文99-36S-6-2

D-준동형사상을 바탕으로 한 드브루인 수열 만들기

(De Bruijn Sequence Generation Based on D-Homomorphism)

宋 翊 鎬 *, 朴 昭 玲 *, 尹 錫 皓 *, 金 洪 吉 *

(Iickho Song, So Ryoung Park, Seokho Yoon, and Hong Gil Kim)

요 약

이 논문에서는 렘펠의 D-준동형사상을 바탕으로 하여 드브루인 수열을 만드는 효과적인 알고리즘을 제안한다. 이 알고리즘에서는 k차 드브루인 수열에서 n차 드브루인 수열의 다음 비트를 만드는데 필요한 배타 논리합 연산수는, r의 2진 표현에서 1의 갯수를 $W(r)$이라 쓸 때, $k(2^{W(n-k)}-1)$쯤임을 보인다: 따라서, 드브루인 함수를 잘 고르면 이 수는 k가 된다.

Abstract

In this paper, an efficient algorithm for generating de Bruijn sequences is presented based on Lempel's D-homomorphism. The number of exclusive-or operations required to generate the next bit for de Bruijn sequences of order n from a de Bruijm function of order k is shown to be approximately $k(2^{W(n-k)}-1)$, where $W(r)$ is the number of one's in the binary representation of r: therefore, the number of required operations can be reduced to k if the de Bruijn function is selected appropriately.

I. 서 론

n차 이진 드브루인 그래프 G_n은 모든 이진 n순서쌍, 곧, 2^n 순서쌍을 꼭지점으로 하고 모서리가 2^{n+1}개인 방향 그래프이다. 꼭지점마다 두 모서리는 $\mathbf{x}=(x_0,x_1,\cdots,x_{n-1})$에서 $\mathbf{y}=(x_1,x_2,\cdots,x_{n-1},y_{n-1})$, $y_{n-1}=0,1$로 이어진다. 드브루인 순환은 G_n의 각 꼭지점을 반드시 그리고 한번씩만 거치는 닫힌 길이다. 서로 다른 드브루인 순환의 갯수는 $2^{2^{n-1}-n}$으로 알려져 있다[1].

* 正會員, 韓國科學技術院 電氣 및 電子工學科
(Department of Electrical Engineering Korea Advanced Institute of Science and Technology)

接受日字:1999年1月22日, 수정완료일:1999年4月29日

드브루인 순환은 주기가 2^n이고 $i=0,1,\cdots,2^n-1$일 때 $\mathbf{s}_i=(s_i,s_{i+1},\cdots,s_{i+n-1})$가 모두 서로 다른 이진 수열 $\{s_i\}$로 나타낼 수 있다. 이러한 수열들을 n차 드브루인 수열이라 부르고, 비선형 귀환 이동 저장기로써 만들 수 있다[2-8]. 드브루인 수열은 난수 특성이 좋고 선형 복잡도가 높기 때문에 흐름 암호의 설계에 많이 쓰인다.

요즈음, 렘펠의 D-준동형사상을 바탕으로 한 드브루인 수열을 만드는 방법이 밝혀졌다[9]. 그러나, 그 방법은 전체 수열을 되풀이하여 만들어내므로 n이 크면 흐름 암호에 실제로 쓰기는 어렵다. 이 논문에서는 렘펠의 D-준동형사상을 바탕으로 하여 드브루인 수열을 만드는 효과적인 알고리즘을 제안한다. 이 알고리즘에서는 k차 드브루인 수열에서 n차 드브루인 수열의 다음 비트를 만드는데 필요한 배타 논리합 연산

수는, r의 2진 표현에서 1의 갯수를 $W(r)$이라 쓸 때, $k(2^{W(n-k)}-1)$쯤임을 보인다.

Ⅱ. 렘펠의 D-준동형사상과 드브루인 수열

$B=\{0,1\}$일 때, n차원 벡터 공간 $B^n=\{(x_1,x_2,\cdots,x_n)\mid x_i\in B, 1\le i\le n\}$을 생각해 보자. B^n에서 $\mathbf{x}=(x_1,\cdots,x_n)$과 $\mathbf{y}=(y_1,\cdots,y_n)$의 이동 관계 $\Rightarrow$를 다음과 같이 정의하며,

$$\mathbf{x}\Rightarrow\mathbf{y} \text{ iff } (x_2,\cdots,x_n)=(y_1,\cdots,y_{n-1}). \quad (1)$$

"$\mathbf{x}$가 $\mathbf{y}$로 움직인다", "$\mathbf{y}$는 $\mathbf{x}$의 바로 뒤 원소이다" 또는 "$\mathbf{x}$는 $\mathbf{y}$의 바로 앞 원소이다" 라고 읽는다. B^n의 모든 원소에 각각 바로 뒤 원소 둘과 바로 앞 원소 둘이 있다. $\mathbf{x}=(x_1,\cdots,x_n)\in B^n$에서 x_i의 이진 보수를 $\overline{x_i}$로 쓸 때, $\overline{\mathbf{x}}=(\overline{x_1},\overline{x_2},\cdots,\overline{x_n})$는 $\mathbf{x}$의 쌍대, $\hat{\mathbf{x}}=(\overline{x_1},x_2,\cdots,x_n)$는 $\mathbf{x}$의 켤레라고 각각 부른다. 그러면, $\overline{\hat{\mathbf{x}}}=\hat{\overline{\mathbf{x}}}$이고, $\mathbf{x}\Rightarrow\mathbf{y}$는 $\overline{\mathbf{x}}\Rightarrow\overline{\mathbf{y}}$와 동치이며, 또한 $\hat{\mathbf{x}}\Rightarrow\mathbf{y}$와도 동치임을 알 수 있다. G_n에서 k-순환은, $i=1,\cdots,k-1$일 때 $\mathbf{x}_k\Rightarrow\mathbf{x}_1$이고 $\mathbf{x}_i\Rightarrow\mathbf{x}_{i+1}$인 서로 다른 k 꼭지점들 $\{\mathbf{x}_1,\mathbf{x}_2,\cdots,\mathbf{x}_k\}$의 닫힌 수열을 말한다. 따라서, 원소가 n개인 $\mathbf{x}_i$의 첫째 비트를 c_i로 쓸 때, 이것을 비트 수열 $\{c_1,c_2,\cdots,c_k\}$로 나타낼 수 있다.

함수 $D:B^n\to B^{n-1}$를 $D(a_1,a_2,\cdots,a_n)=(a_1\oplus a_2, a_2\oplus a_3,\cdots,a_{n-1}\oplus a_n)$으로 정의하면, D가 2대 1 전사 함수임은 쉽게 알 수 있다. 함수 D는 이동 관계를 보존하므로 G_n의 G_{n-1}위로의 그래프 준동형사상이다[2]. 또한, G_n에서 k-순환 Γ의 1의 갯수가 짝수이면, Γ는 함수 D에 대하여 k-순환 $C=\{c_1,\cdots,c_k\}$와 $\overline{C}=\{\overline{c_1},\cdots,\overline{c_k}\}$의 상이 되고 그 역도 성립함이 알려져 있다[2]. G_n에서 2^n-순환의 1의 수는 2^{n-1}임이 잘 알려져 있으므로, 2^n-순환은 함수 D에 대하여 G_{n+1}의 서로 다른 한 쌍의 순환 C와 $\overline{C}$의 원상이다. 한편, x가 C_1에 있고 $\hat{x}$가 C_2에 있을 때, x와 $\hat{x}$의 바로 뒤 원소를 서로 바꾸면 C_1과 C_2를 하나의 순환으로 만들 수 있기 때문에[5], x가 C에 있고 $\hat{x}$가 $\overline{C}$에 있는 켤레쌍 x와 $\hat{x}$를 찾을 수 있다면 두 순환 C와 $\overline{C}$를 하나의 순환으로 만들 수 있다.

이제 $e_1=0$이고 $e_{i+1}=\overline{e_i}$, $i=1,\cdots,n-1$인 꼭지점 $e=(e_1,\cdots,e_n)$를 생각해 보자. 이때, e가 C에 있으면, $\overline{e}$은 반드시 $\overline{C}$에 있고 그 역도 성립한다. 또한 $e\Rightarrow\hat{e}$이므로 e와 $\hat{e}$는 켤레쌍이다. 그러므로, 다음의 정리를 이끌어 낼 수 있다. 앞으로는 n차 드브루인 수열을 만드는 함수를 n차 드브루인 수열 함수라고 부르기로 하자.

정 리 1[2] ϕ를 $(n-1)$차 드브루인 수열 함수라 하고, h를 다음과 같이 정의하자.

$$h(x_1,\cdots,x_n)=x_n\oplus\phi(x_1\oplus x_2,x_2\oplus x_3,\cdots,x_{n-1}\oplus x_n)\oplus x_2^{e_2}x_3^{e_3}\cdots x_n^{e_n}. \quad (2)$$

여기서, $e_2=1$, $e_{i+1}=\overline{e_i}$, $i=2,\cdots,n-1$이고, $x_i^0=\overline{x_i}$이다. 그러면, h는 n차 드브루인 수열 함수이다.

Ⅲ. 드브루인 수열을 만드는 알고리즘

n이 크지 않을 때는 정리 1을 써서 차수가 낮은 드브루인 수열 함수에서 차수가 더 높은 드브루인 수열 함수를 얻을 수 있다. 그러나, n이 크면, 정리 1을 되풀이하여 차수가 낮은 드브루인 수열 함수에서 n차 드브루인 수열 함수를 얻어 내는 것이 매우 어렵게 된다. 이제, 드브루인 수열 함수를 되풀이하여 계산하지 않고도 차수가 낮은 드브루인 수열 함수에서 차수가 높은 드브루인 수열을 만들어내는 알고리즘을 생각해 보자.

먼저, 함수 D를 효과적으로 계산하는 방법을 생각해 보자.

정 리 2 음이 아닌 정수 n이 있을 때, $m=2^n$이라 하면

$$D^m(x_1,x_2,\cdots,x_{m+1})=x_1\oplus x_{m+1} \quad (3)$$

이다.

증 명: $(1\oplus x)^n=1\oplus x^m$을 쓰면 쉽게 증명됨.

정 리 3 m이 2의 거듭제곱이고 $n>m$이라면

$$D^m(x_1,x_2,\cdots,x_n)=(x_1\oplus x_{m+1},x_2\oplus x_{m+2},\cdots,x_{n-m}\oplus x_n). \quad (4)$$

증 명: 정리 2를 쓰면 쉽게 증명됨.

정 리 4 $r=r_1+r_2+\cdots+r_k$라 하자. 여기서 r_i는 2의 거듭제곱이다. 그리고, $E_i(x_{j1}\oplus x_{j2}\oplus\cdots)=x_{j_1}\oplus x_{j_1+i}\oplus x_{j_2}\oplus x_{j_2+i}\oplus\cdots$ 이라 정의하면

$$\begin{aligned}&D^r(x_1,x_2,\cdots,x_n)\\&=D^{r_k}\cdots D^{r_1}(x_1,x_2,\cdots,x_n)\\&=(E_{r_k}\cdots E_{r_1}(x_1),E_{r_k}\cdots E_{r_1}(x_2),\cdots,E_{r_k}\cdots E_{r_1}(x_{n-r})).\end{aligned}\tag{5}$$

증 명: 정리 3을 쓰면 쉽게 증명됨.

정리 4에서 $r=n-1$이면, $D^r(x_1,x_2,\cdots x_n)=E_{r_k}\cdots E_{r_1}(x_1)$인데 이는 정리 2가 일반화된 것이다. 보기로 D^{100}을 생각해 보자. $100=2^6+2^5+2^2=64+32+4$ 이므로,

$$\begin{aligned}&D^{100}(x_1,\cdots,x_{101})\\&=D^4\cdot D^{32}\cdot D^{64}(x_1,\cdots,x_{101})\\&=D^4\cdot D^{32}(x_1\oplus x_{65},x_2\oplus x_{66},\cdots,x_{37}\oplus x_{101})\\&=D^4(x_1\oplus x_{65}\oplus x_{33}\oplus x_{97},\cdots,x_5\oplus x_{69}\oplus x_{37}\oplus x_{101})\\&=x_1\oplus x_5\oplus x_{33}\oplus x_{37}\oplus x_{65}\oplus x_{69}\oplus x_{97}\oplus x_{101}\end{aligned}\tag{6}$$

이다. 정리 4에서 $D^r(x_1,\cdots,x_n)$를 계산하는데 필요한 배타 논리합 연산수는 $(2^{W(r)}-1)(n-r)$ 임을 쉽게 알 수 있다.

이제, $S:B^n\to B^n$를 왼쪽 이동 함수

$$S((x_1,x_2,\cdots,x_n))=(x_2,x_3,\cdots,x_n,0)\tag{7}$$

로, 그리고 $P_i:B^n\to B$를 비트 선택 함수

$$P_i((x_1,x_2,\cdots,x_n))=x_i,\quad 1\le i\le n.\tag{8}$$

로 놓으면, 다음의 성질들을 쉽게 얻을 수 있다.

성 질 1 $\mathbf{x}=(x_1,x_2,\cdots,x_n)$와 $\mathbf{y}=(y_1,y_2,\cdots,y_n)$가 B^n의 원소일 때,

i) $S(\mathbf{x}\oplus\mathbf{y})=S(\mathbf{x})\oplus S(\mathbf{y})$,

ii) $P_i(\mathbf{x}\oplus\mathbf{y})=P_i(\mathbf{x})\oplus P_i(\mathbf{y}),\quad 1\le i\le n$,

iii) $D\cdot S(\mathbf{x})=S\cdot D(\mathbf{x})\oplus(0,0,\cdots,0,x_n)$,

곧, $D\cdot S(\mathbf{x})=S\cdot D(\mathbf{x}),\quad 1\le i\le n-2$,

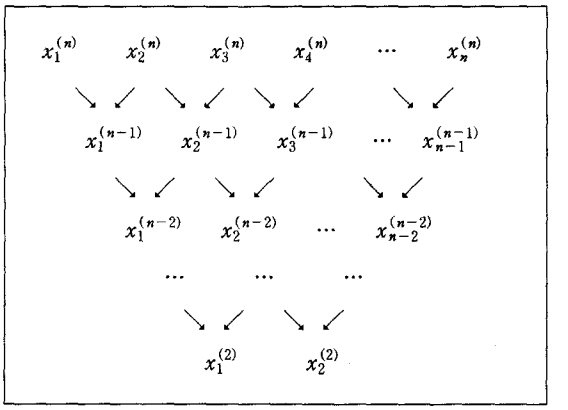
$P_{n-1}\cdot D\cdot S(\mathbf{x})=x_n,\quad P_{n-1}\cdot S\cdot D(\mathbf{x})=0$,

iv) $P_i(\mathbf{x})=P_{i-1}\cdot S(\mathbf{x}),\quad 1\le i\le n-1$,

v) $P_i\cdot D(\mathbf{x})=P_i(\mathbf{x})\oplus P_{i+1}(\mathbf{x}),\quad 1\le i\le n-1$

이 성립한다.

이제, $2\le j\le i,\ 2\le i\le n-1$일 때, $\mathbf{x}^{(i)}=(x_1^{(i)},x_2^{(i)},\cdots,x_i^{(i)})\in B^i,\quad i=n,n-1,\cdots,1,\ x_j^{(i)}=x_j^{(i+1)}\oplus x_{j+1}^{(i+1)}$라 하면, 다음 상자 안에 보인 방법과 $P_i\cdot D^j(\mathbf{x}^{(n)})=x_i^{(n-j)},\ 1\le j\le i$로부터 아래 정리 5를 얻는다.



정 리 5 $i\in\{1,2,\cdots,n\}$가 정수일 때,

$$\begin{aligned}&P_{n-i}\cdot D^i\cdot S(\mathbf{x}^{(n)})\\&\quad=x_n^{(n)}\oplus x_{n-1}^{(n-1)}\oplus\cdots\oplus x_{n-i+1}^{(n-i+1)}\end{aligned}\tag{9}$$

이다.

증 명: 수학적 귀납법으로 증명하자. $i=1$이면 (12)가 뚜렷이 성립한다. 이제, $i=k$에서 (9)가 성립한다고 두면, 곧,

$$\begin{aligned}&P_{n-k}\cdot D^k\cdot S(\mathbf{x}^{(n)})\\&\quad=x_n^{(n)}\oplus x_{n-1}^{(n-1)}\oplus\cdots\oplus x_{n-k+1}^{(n-k+1)}\end{aligned}\tag{10}$$

이면,

$$\begin{aligned}&x_n^{(n)}\oplus x_{n-1}^{(n-1)}\oplus\cdots\oplus x_{n-k+1}^{(n-k+1)}\oplus x_{n-k}^{(n-k)}\\&\quad=P_{n-k}\cdot D^k\cdot S(\mathbf{x}^{(n)})\oplus x_{n-k}^{(n-k)}\\&\quad=P_{n-k}\cdot D^k\cdot S(\mathbf{x}^{(n)})\oplus P_{n-k-1}\cdot D^k\cdot S(\mathbf{x}^{(n)})\end{aligned}$$

$$= P_{n-k-1} \cdot D^{k+1} \cdot S(\mathbf{x}^{(n)}) \tag{11}$$

이므로 $i=k+1$에서도 (9)가 성립한다. (증명 끝)

이제, $R: B^n \to B^{n-1}$를 끊음 함수

$$R((x_1, x_2, \cdots, x_n)) = (x_1, x_2, \cdots, x_{n-1}) \tag{12}$$

로 놓으면, 성질 1로부터 다음을 얻는다.

성 질 2 $\mathbf{x} \in B^n$일 때,

i) $R \cdot S \cdot D(\mathbf{x}) = R \cdot D \cdot S(\mathbf{x})$,

ii) $R \cdot D(\mathbf{x}) = D \cdot R(\mathbf{x})$,

iii) $R \cdot S \cdot D(\mathbf{x}) = D \cdot R \cdot S(\mathbf{x})$.

이제, B^n의 특수한 원소 몇몇을 다음과 같이 쓰자.

$$\mathbf{0} = (\overbrace{0,0,0,0,\cdots}^{n}), \tag{13}$$

$$\mathbf{5} = (\overbrace{1,0,1,0,\cdots}^{n}), \tag{14}$$

$$\mathbf{a} = (\overbrace{0,1,0,1,\cdots}^{n}), \tag{15}$$

$$\mathbf{f} = (\overbrace{1,1,1,1,\cdots}^{n}). \tag{16}$$

그러면, 다음의 식이 성립함을 쉽게 보일 수 있다.

$$D(\mathbf{0}) = \mathbf{0} \in B^{n-1}, \tag{17}$$

$$D(\mathbf{5}) = \mathbf{f} \in B^{n-1}, \tag{18}$$

$$D(\mathbf{a}) = \mathbf{f} \in B^{n-1}, \tag{19}$$

$$D(\mathbf{f}) = \mathbf{0} \in B^{n-1}. \tag{20}$$

$\mathbf{x} \in B^n$일 때 $U: B^n \to B$를

$$U(\mathbf{x}) = \begin{cases} 1, & \mathbf{x} = \mathbf{5} \text{ 일 때,} \\ 0, & \text{그 밖에} \end{cases} \tag{21}$$

로 놓자. 그러면, 함수 $U(\mathbf{x})$를 다음과 같이 나타낼 수 있다.

$$U(\mathbf{x}) = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}. \tag{22}$$

여기서, $e_1 = 1$, $e_{i+1} = \overline{e_i}$, $i = 1, 2, \cdots, n-1$이고, $x_i^0 = \overline{x_i}$이다.

성 질 3 $\mathbf{x} \in B^n$일 때,

i) $D(\mathbf{x}) = \mathbf{0}$ 과 $\mathbf{x} = \mathbf{0}$ 또는 $\mathbf{x} = \mathbf{f}$ 는 동치이다

ii) $D(\mathbf{x}) = \mathbf{f}$ 과 $\mathbf{x} = \mathbf{5}$ 또는 $\mathbf{x} = \mathbf{a}$ 는 동치이다

iii) 만약 $D^i(\mathbf{x}) = \mathbf{a}$인 i, $0 \le i \le n-2$가 있다면, 모든 j, $0 \le j \le n-2$에 대하여 $U \cdot D^j(\mathbf{x}) = 0$이다.

iv) 만약 $D^i(\mathbf{x}) = \mathbf{5}$인 i, $0 \le i \le n-2$가 있다면, 모든 j $0 \le j \le n-2$, $j \ne i$에 대하여 $U \cdot D^j(\mathbf{x}) = 0$이다.

v) 만약 $D^i(\mathbf{x}) = \mathbf{0}$, $\mathbf{x} \ne \mathbf{0}$, $\mathbf{x} \ne \mathbf{f}$이면, $D^j(\mathbf{x}) = \mathbf{5}$ 또는 $D^j(\mathbf{x}) = \mathbf{a}$인 j, $0 \le j \le i-1$가 존재한다.

정 의 1 양수 $i < n$이 있을 때, B^n에서 B로의 함수 Δ_i^n을 다음과 같이 정의한다.

$$\Delta_i^n(\mathbf{x}) = U(\mathbf{x}) \oplus U(D(\mathbf{x})) \oplus U(D^2(\mathbf{x})) \oplus \cdots \oplus U(D^{n-i-1}(\mathbf{x})). \tag{23}$$

성질 3에서, $\Delta_i^n(\mathbf{x})$가 1이면 (23)의 오른쪽 식에서 오직 한 항만이 1임을 쉽게 보일수 있다: $U(\mathbf{x}) = 1$이면 $\mathbf{x} = \mathbf{5}$이고 그 역도 성립하며, 둘 이상의 항이 함께 1이 될 수 없기 때문이다. $\Delta_i^n(\mathbf{x})$를 계산하는 방법이 아래 델타 알고리즘으로 나타나 있다: 단계 3과 4는 각각 성질 3의 ii)와 v)를 바탕으로 한다. 단계 5-10은 성질 3을 써서 $D^r(\mathbf{x}) = \mathbf{5}$ 또는 $\mathbf{a}$를 찾아낸다.

델타 알고리즘

단 계 0. n, i, $\mathbf{x}$ 를 입력.

단 계 1. $\mathbf{x} = \mathbf{5}$이면, $\Delta_i^n(\mathbf{x}) := 1$이다. 빠져 나감.
$\mathbf{x} = \mathbf{a}$이거나, $\mathbf{x} = \mathbf{f}$ 또는 $\mathbf{x} = \mathbf{0}$이면,
$\Delta_i^n(\mathbf{x}) := 0$이다. 빠져 나감.

단 계 2. $d := n - i + 1$

단 계 3. $D^d(\mathbf{x}) \ne \mathbf{0}$이면, $\Delta_i^n(\mathbf{x}) := 0$이다.
빠져 나감.

단 계 4. $k := 1$, $m = d - 1$

단 계 5. $k \le m$인 동안 다음을 실행한다.

단 계 6. $t := \lfloor \frac{k+m}{2} \rfloor$

단 계 7. 만약 $D^t(\mathbf{x}) = \mathbf{5}$이면, $\Delta_i^n(\mathbf{x}) := 1$이다.
빠져 나감.

단 계 8. 만약 $D^t(\mathbf{x})=\mathbf{a}$이면, $\Delta_i^n(\mathbf{x}) := 0$이다.
빠져 나감.
단 계 9. 만약 $D^t(\mathbf{x})=\mathbf{0}$이면 $m := t-1$이고,
그렇지 않으면 $k := t$이다.
단 계 10. 끝

이제, (2)를 아래와 같이 써 보자.

$$h_n(\mathbf{x}) = x_n \oplus h_{n-1}(D(\mathbf{x})) \oplus U\cdot R\cdot S(\mathbf{x}), \quad (24)$$

여기서, $\mathbf{x}=(x_1,\cdots,x_n)$이다. 이제, 다음과 같이 (24)를 거듭 써서 h_2에서 h_n을 계산할 수 있다.

$$h_n(\mathbf{x}^{(n)}) = x_n^{(n)} \oplus h_{n-1}(D(\mathbf{x}^{(n)})) \oplus U\cdot R\cdot S(\mathbf{x}^{(n)})$$

$$h_{n-1}(D(\mathbf{x}^{(n)})) = x_{n-1}^{(n-1)} \oplus h_{n-2}(D^2(\mathbf{x}^{(n)})) \oplus U\cdot R\cdot S\cdot D(\mathbf{x}^{(n)})$$

$$h_{n-2}(D^2(\mathbf{x}^{(n)})) = x_{n-2}^{(n-2)} \oplus h_{n-3}(D^3(\mathbf{x}^{(n)})) \oplus U\cdot R\cdot S\cdot D^2(\mathbf{x}^{(n)})$$

$$\vdots \qquad \vdots$$

$$h_3(D^{n-3}(\mathbf{x}^{(n)})) = x_3^{(3)} \oplus h_2(D^{n-2}(\mathbf{x}^{(n)})) \oplus U\cdot R\cdot S\cdot D^{n-3}(\mathbf{x}^{(n)}).$$

정리 3, 성질 2, 그리고 Δ_i^n 의 정의에서 다음을 얻을 수 있다.

$$\begin{aligned} h_n(\mathbf{x}^{(n)}) &= x_n^{(n)} \oplus x_{n-1}^{(n-1)} \oplus \cdots \oplus x_3^{(3)} \oplus h_2(D^{n-2}(\mathbf{x}^{(n)})) \\ &\quad \oplus U\cdot R\cdot S(\mathbf{x}^{(n)}) \oplus U\cdot R\cdot S\cdot D(\mathbf{x}^{(n)}) \\ &\quad \oplus \cdots \oplus U\cdot R\cdot S\cdot D^{n-3}(\mathbf{x}^{(n)}) \qquad (25) \\ &= P_2\cdot D^{n-2}\cdot S(\mathbf{x}^{(n)}) \oplus h_2(D^{n-2}(\mathbf{x}^{(n)})) \\ &\quad \oplus \Delta_1^{n-1}(R\cdot S(\mathbf{x}^{(n)})). \end{aligned}$$

위는 다음 정리 6의 증명인 셈이다.

정 리 6 함수 h_2를 2차 드브루인 수열 함수라 하면, $\mathbf{x}^{(n)}\in B^n$일 때,

$$h_n(\mathbf{x}^{(n)}) = P_2\cdot D^{n-2}\cdot S(\mathbf{x}^{(n)}) \oplus h_2(D^{n-2}(\mathbf{x}^{(n)})) \oplus \Delta_1^{(n-1)}(R\cdot S(\mathbf{x}^{(n)})) \quad (26)$$

은 n차 드브루인 수열 함수이다.

또한, 정리 6을 일반화하면 다음 정리 7을 얻을 수 있다.

정 리 7 함수 h_k를 k차 드브루인 수열 함수라 하면, $\mathbf{x}^{(n)}\in B^n$일 때,

$$h_n(\mathbf{x}^{(n)}) = P_k\cdot D^{n-k}\cdot S(\mathbf{x}^{(n)}) \oplus h_k(D^{n-k}(\mathbf{x}^{(n)})) \oplus \Delta_{k-1}^{n-1}(R\cdot S(\mathbf{x}^{(n)})) \quad (27)$$

은 n차 드브루인 수열 함수이다.

정리 7을 쓰면, 함수 $h_n(\mathbf{x})$을 구체적으로 계산하지 않고도 차수가 낮은 드브루인 수열에서 n차 드브루인 수열의 다음 비트를 얻을 수 있다.

델타 알고리즘이 얼마나 복잡한지 알아보자. 이 알고리즘에서 단계 5 - 10은 이진 탐색 루프이다. 단계 3에서 $D^{n-i+1}(\mathbf{x})\neq 0$라면, $\Delta_i^n(\mathbf{x})=0$이고, 알고리즘은 끝난다. D-준동형사상이 2대 1 함수이므로, D^{n-i+1}는 2^{n-i+1}대 1 함수이다. 곧, $D^{n-i+1}(\mathbf{x})=0$인 B^n의 원소 $\mathbf{x}$의 갯수는 2^{n-i+1}이고, 단계 3에서 알고리즘이 끝나지 않을 확률은 $\frac{2^{n-i+1}}{2^n} = \frac{1}{2^{i-1}}$이다. 그러므로, 단계 3에서 (이 단계에서 $D^{n-k+1}(\mathbf{x})$을 계산한다) 알고리즘이 끝날 확률은 $1-\frac{1}{2^{i-1}}$이다. (보기를 들어, 11차 드브루인 수열 함수에서 100차 드브루인 수열을 만든다고 생각해 보자. 이 때, 단계 3에서 이 알고리즘이 끝날 확률은 1023/1024≈99.9%이다. 물론 드브루인 수열 함수의 차수가 더 크다면, 그 확률도 더 높다.)

따라서, k가 10보다 크면 식 (27)에서 h_n을 계산할 때 $D^r(\mathbf{x})$를 세 번만 계산하면 넉넉할 확률이 매우 높다 (D^{n-k+1}계산 한 번, $D^{n-k}(\mathbf{x})$계산 두 번). $D^r(\mathbf{x})$를 계산하는데 필요한 배타 논리합 연산수가 $(2^{W(r)}-1)(n-r)$라는 것을 생각하면 k차 드브루인 수열 함수에서 n차 드브루인 수열의 다음 비트를 만드는데 필요한 배타 논리합 연산수는 $N_e = k(2^{W(n-k)}-1)+k(2^{W(n-k)}-1)+(k-1)(2^{W(n-k+1)}-1)$

라는 것을 쉽게 알 수 있다. $2^{W(r)}-1 \le r$이므로 이 수 N_e는 $k(n-k)+k(n-k)+(k-1)(n-k+1)$ 보다 작거나 같게 된다. 좀 더 느슨하게는 $N_e \le 3k(n-k+1)$이다.

다음 정리 8을 써서 D^r을 한 번에 계산할 수 있다.

정 리 8 $\mathbf{x}^{(n)} = (x_1^{(n)}, x_2^{(n)}, \cdots, x_n^{(n)})$, $\mathbf{y} = (x_1^{(n)}, x_2^{(n)}, \cdots, x_n^{(n)}, 0)$, $\Gamma = D^{n-k}(\mathbf{y})$라고 하면

i) $D^{n-k}(\mathbf{x}^{(n)}) = R(\Gamma)$,

ii) $D^{n-k} \cdot S(\mathbf{x}^{(n)}) = R \cdot S(\Gamma)$,

iii) $D^{n-k+1} \cdot R \cdot S(\mathbf{x}^{(n)}) = R \cdot S \cdot R \cdot D(\Gamma)$.

증 명:

i) 성질 2의 ii)로부터, $D^{n-k} \cdot R(\mathbf{y}) = R \cdot D^{n-k}(\mathbf{y})$. 그러므로, $D^{n-k}(\mathbf{x}^{(n)}) = D^{n-k} \cdot R(\mathbf{y}) = R \cdot D^{n-k}(\mathbf{y}) = R(\Gamma)$.

ii) $R \cdot S(\mathbf{y}) = S \cdot R(\mathbf{y})$이고, $R(\mathbf{y}) = \mathbf{x}^{(n)}$이므로, $D^{n-k} \cdot S(\mathbf{x}^{(n)}) = D^{n-k} \cdot S \cdot R(\mathbf{y}) = D^{n-k} \cdot R \cdot S(\mathbf{y})$이다. 따라서, 성질 2의 iii)으로부터 $D^{n-k} \cdot S(\mathbf{x}^{(n)}) = R \cdot S(\Gamma)$이다.

iii) 성질 2의 iii)으로부터, $D^{n-k+1} \cdot R \cdot S(\mathbf{x}^{(n)}) = R \cdot S \cdot D \cdot D^{n-k}(\mathbf{x}^{(n)}) = R \cdot S \cdot D \cdot R(\Gamma)$. (증명끝)

이제, 정리 8에서, $D^{n-k}(\mathbf{y})$을 한 번만 계산하면 식 (27)의 $D^{n-k}(\mathbf{x}^{(n)})$, $D^{n-k} \cdot S(\mathbf{x}^{(n)})$, $\Delta_{k-1}^{n-1}(R \cdot S(\mathbf{x}^{(n)}))$을 얻을 수 있음을 알 수 있다. 그러므로 이 때 필요한 비트 배타 논리합 연산수는 $k(2^{W(n-k)}-1)$쯤 되는데, 이 수는 N_e의 1/3쯤 이다. 이 때, $W(n-k)=1$이 되는 드브루인 함수의 차수 k를 고르면, 이 수는 다시 k로 줄어든다. 여기서, k가 정해지면 k차 드브루인 함수는 순환적이므로 쉽게 찾아서 쓸 수 있다. 보기를 들면, $n=50=110010_2$이면 $k=10010_2=18$ 인데, $W(18-2)=1$이므로, 18차 드브루인 함수는 다시 2차 드브루인 함수로 쉽게 계산할 수 있다.

Ⅳ. 맺 음 말

이 논문에서는, D-준동형사상을 바탕으로 하여 드브루인 수열을 만드는 효과적인 알고리즘을 하나 생각해 보았다. 정리 1에서 $x_2^1 x_3^0 x_4^1 x_5^0 \cdots x_n^a$ 항을 $x_2^0 x_3^1 x_4^0 x_5^1 \cdots x_n^b$로 바꿀 수 있음을 눈여겨 보아야 한다. 제안한 알고리즘을 쓰면 차수가 낮은 드브루인 함수에서 차수가 높은 드브루인 수열을 효율적으로 만들 수 있고, 드브루인 수열의 차수를 잘 고르면 계산량을 훨씬 더 줄일 수 있다.

부 록

표 1. $k=2,3,4$일 때 k차 드브루인 수열 함수

Table 1. De Bruijn sequence function of order k when $k=2,3,4$.

k	k차 드브루인 수열 함수의 결과
2	{1,0,1,0}
3	{1,0,1,0,0,1,1,0}
	{1,0,0,1,1,0,1,0}
4	{1,0,0,1,0,1,0,1,1,0,1,0,0,1,0,1}
	{1,0,0,1,0,1,1,0,1,0,1,0,0,1,1,0}
	{1,0,0,1,1,0,0,1,0,1,1,0,1,0,1,0}
	{1,0,0,1,1,0,0,1,1,0,0,1,1,0,1,0}
	{1,0,0,1,1,0,0,1,1,0,1,0,0,1,1,0}
	{1,0,0,1,1,0,1,0,0,1,1,0,0,1,1,0}
	{1,0,0,1,1,0,1,0,1,0,0,1,0,1,1,0}
	{1,0,0,1,1,0,1,0,1,0,1,0,1,0,1,0}
	{1,0,1,0,0,1,0,1,0,1,1,0,1,0,1,0}
	{1,0,1,0,0,1,1,0,0,1,1,0,0,1,1,0}
	{1,0,1,0,1,0,0,1,0,1,0,1,1,0,1,0}
	{1,0,1,0,1,0,0,1,0,1,1,0,0,1,1,0}
	{1,0,1,0,1,0,0,1,1,0,1,0,1,0,1,0}
	{1,0,1,0,1,0,1,0,0,1,0,1,0,1,1,0}
	{1,0,1,0,1,0,1,0,0,1,1,0,1,0,1,0}
	{1,0,1,0,1,0,1,0,1,0,1,0,0,1,1,0}

표 1은 $k=2,3,4$일 때 k차 드브루인 수열 함수, $F(x_1, \cdots, x_k)$의 출력이다. 이 표에서 출력은 $(x_1, \cdots, x_k)$

를 십진법으로 쓴 것, 곧, $\sum_{i=0}^{k-1} x_i 2^i$이다. 보기를 들어, {1,0,1,0}는 $F(0,0)=1$, $F(1,0)=0$, $F(0,1)=1$, $F(1,1)=0$을 뜻한다.

참 고 문 헌

[1] N.G. de Bruijn, "A Combinatorial Problem," *Nederl. Akad. Wetensch. Proc.*, vol. 49, pp. 758-764, 1946.

[2] A. Lempel, "On a Homomorphism of the De Bruijn Graph and Its Applications to the Design of Feedback Shift Registers," *IEEE Trans. Computers*, vol. 19, pp. 1204-1209, Dec. 1970.

[3] A. Lempel, "Cryptology in Transition," *Computing Surveys*, vol. 11, pp. 285-303, Dec. 1979.

[4] S.W. Golomb, *Shift Register Sequences*, Aegean Park Press, Laguna Hills, CA, 1982.

[5] H. Fredrickson, "A Survey of Full Cycle Algorithms," *SIAM Review*, vol. 24, pp. 195-221, April 1982.

[6] A.H. Chan, R.A. Games, and E.L. Key, "On the Complexities of de Bruijn Sequences," *J. Comb. Theory, Ser. A*, vol. 33, pp. 233-246, Nov. 1982.

[7] T. Helleseth and T. Klove, "The Number of Cross-Join Pairs in Maximum Length Linear Sequences", *IEEE Trans. Inform. Theory*, vol. 37, pp. 1731-1733, Nov. 1991.

[8] T. Chang, I. Song, H.M. Kim, and S.H. Cho, "Cross-Joins in de Bruijn Sequences and Maximum Length Linear Sequences", *IEICE Trans. Fundamentals*, vol. E76A, pp. 1494-1501, Sep. 1993.

[9] F.S. Annexstein, "Generating De Bruijn SequencesAn Efficient Implementation", *IEEE Trans. Computers*, vol. 46, pp. 198-200, Feb. 1997.

[10] S. Baase, *Computer Algorithms: Introduction to Design and Analysis*, Addison-Wesley, Reading, MA, 1978.

저 자 소 개

宋 翊 鎬(正會員)

1960년 2월 20일 태어남. 1978년 3월 ~ 1982년 2월 서울대학교 전자공학과 공학사 (준최우등). 1982년 3월 ~ 1984년 2월 서울대학교 전자공학과 공학석사. 1984년 1월 ~ 1985년 8월 펜실베니아대학교 전기공학과 공학석사. 1985년 9월 ~ 1987년 5월 펜실베니아대학교 전기공학과 공학박사. 1987년 3월 ~ 1988년 2월 벨 통신연구소 연구원. 1988년 3월 ~ 1991년 8월 한국과학기술원 전기 및 전자공학과 조교수. 1991년 9월 ~ 1998년 8월 한국과학기술원 전기 및 전자공학과 부교수. 1998년 9월 ~ 현재 한국과학기술원 전기 및 전자공학과 교수. 1995년 1월 ~ 현재 한국통신학회 논문지 편집위원. 1996년 1월 ~ 현재 한국음향학회 영문논문지 편집위원. 1998년 1월 ~ 현재 Journ. Comm., Networks 편집위원. 1991년 11월, 1996년 11월 한국통신학회 학술상 받음. 1993년 11월 한국음향학회 우수연구상 받음. 1998년 11월 한국통신학회 LG학술상 받음. 대한전자공학회, 한국음향학회, 한국통신학회 평생회원; IEE 회원; IEEE 선임회원. 주관심분야는 통계학적 신호처리와 통신이론, 신호검파와 추정, 이동통신

尹 錫 皓(正會員)

1976년 1월 7일 태어남. 1993년 3월 ~ 1997년 2월 한국과학기술원 전기 및 전자공학과 공학사 (최우등). 1997년 3월 ~ 1999년 2월 한국과학기술원 전기 및 전자공학과 공학석사. 1999년 3월 ~ 현재 한국과학기술원 전기 및 전자공학과 박사과정. 주관심분야는 이동통신, 통계학적 신호처리, 적응 신호처리

朴 昭 玲(正會員)

1974년 11월 22일 태어남. 1993년 3월 ~ 1997년 2월 연세대학교 전자공학과 공학사. 1997년 3월 ~ 1999년 2월 한국과학기술원 전기 및 전자공학과 공학석사. 1999년 3월 ~ 현재 한국과학기술원 전기 및 전자공학과 박사과정. 주관심분야는 이동통신, 신호검파

金 洪 吉(正會員)

1972년 7월 20일 태어남. 1991년 3월 ~ 1995년 2월 한양대학교 전자통신공학과 공학사. 1995년 3월 ~ 1997년 2월 한국과학기술원 전기 및 전자공학과 공학석사. 1997년 3월 ~ 현재 한국과학기술원 전기 및 전자공학과 박사과정. 주관심분야는 이동통신, 검파이론