Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.4.447

의사-제어된 NCV 게이트로 실현된 매크로 양자회로의 새로운 함수 합성법

박동영* · 정연만**

A New Functional Synthesis Method for Macro Quantum Circuits Realized in Affine-Controlled NCV-Gates

Dong-Young Park* · Yeon-Man Jeong**

요 약

최근에 양자회로 합성과 관련한 대부분의 방법들은 컴퓨터 시뮬레이션에 적합한 서술적 표현 구조를 채택하고 있어 합성된 양자함수들에 대한 분석이 어렵다. 본 논문에서는 구조가 단순하고 직관적 사고가 가능한 양자회로의 새로운 함수표현법을 제안한다. 본 논문 제안사항은 타깃라인상의 유니터리 연산자들의 직렬 적 행렬연산을 멱함수의 산술연산과 modulo 2 연산이란 수학적 치환을 통해 유니터리 연산자의 제어입력을 자신의 멱함수로 합성하는 새로운 함수합성에 있다. 본 논문의 함수합성 알고리듬은 의사-제어된 NCV-양자게이트를 이용한 가역 및 비가역 양자회로들의 함수표현과 새로운 함수합성에 유용하다.

ABSTRACT

Recently most of functional synthesis methods for quantum circuit realization have a tendency to adopt the declarative functional expression more suitable for computer algorithms, so it's difficult to analysis synthesized quantum functions. This paper presents a new functional representation of quantum circuits compatible with simple architecture and intuitive thinking. The proposal of this paper is a new functional synthesis development by using the control functions as the power of corresponding to affine-controlled quantum gates based on the mathematical substitution of serial-product matrix operation over the target line for the arithmetic and modulo-2 ones between power functions of unitary operators. The functional synthesis algorithm proposed in this paper is useful for the functional expressions and synthesis using both of reversible and irreversible affine-controlled NCV-quantum gates.

키워드

Functional Representation, Functional Synthesis, Quantum Circuits, NCV-Quantum Gate, Affine-Controlled
함수 표현, 함수 합성, 양자 회로, 엔씨브이-양자 게이트 , 의사-제어된

Ⅰ. 서 론

최근 가역 논리(reversible logic)회로의 에너지 무손실(energy lossless)이란 잠재적 성질 때문에 전 세계적으로 이와 관련된 다양한 연구가 진행되고 있다. 고전적 비가역 회로를 가역 회로로 바꿔주는 대표적 양자게이트로는 MCT(multiple-controlled-Toffoli)로 불리는 다중제어-NOT 기능의 Toffoli 게이트가 유명

* 강릉원주대학교 정보통신공학과(kouksundo@gwnu.ac.kr)
** 교신저자(corresponding author) : 강릉원주대학교 정보통신공학과(ymjeong@gwnu.ac.kr)
접수일자 : 2014. 02. 17 심사(수정)일자 : 2014. 03. 21 게재확정일자 : 2014. 04. 11

하다. 그 외에 가역논리에서 함수 합성에 주로 사용하는 주요 양자게이트 들로는 단일 controlled-NOT 기능을 갖는 Feynman 게이트, 3-입력 Toffoli 게이트와 Feynman 게이트 기능을 합성한 Peres 게이트, 제어 신호에 의해 인접 라인의 비트 정보와 바꿀 수 있는 Fredkin 게이트 등이 있다. 이와 같은 매크로 게이트들의 실현은 NOT, controlled-NOT, controlled-root-of-NOT과 같은 NCV-군(family) 의사(affine) 게이트들의 양자논리에 근거한 수학적 실현과 실제의 물리적 실현으로 구분할 수 있다. 양자 게이트의 실현에서 가장 비용이 적게 들고 고전적 회로, 가역회로 및 양자회로 모두에 사용할 수 있는 선형적 특성의 의사 게이트는 NOT 게이트와 controlled-NOT 게이트뿐이다. 특히 controlled-root-of-NOT 게이트라 불리는 V-게이트 군은 양자 얽힘(entanglement)이라는 고전 역학에서는 불가능한 비가역적 특성이 발생할 수 있으므로 타깃 라인 상의 제한적 실현을 통해 가역적 특성을 유지도록 설계하는 경향이다[1]. 그 동안 매크로 레벨의 양자게이트를 더 작은 레벨의 양자게이트들에 의해 합성하고 실현하기 위한 다양한 연구 노력들이 있었다. 이와 같은 연구과정에 필연적으로 발생하는 양자회로의 함수표현과 관련한 일반적 방법은 없다. 본 논문에서는 최근 사용되고 있는 양자회로의 몇 가지 함수 표현법들[1-5]는 수식이라기보다는 컴퓨터 언어에 가까운 구조를 보여주고 있어 직관적 분석과 이해가 어려운 점을 감안하여 서로 다른 의사 게이트 함수들의 수학적 특성을 보전하면서도 단일 수식으로의 함수합성이 가능한 새로운 함수표현법을 제안하게 되었다. 본 연구의 범위는 양자게이트의 물리적 실현이 아닌 수학적 논리적 실현에 국한한다.

본 논문의 구성은 2장에서 양자 논리의 배경 이론을 논한 후에 3장에서 기존의 양자회로 함수표현 방법을 고찰하였다. 4장에서는 본 논문의 새로운 함수표현과 합성 알고리듬을 제안하였고, 5장에서는 본 논문 방법을 기존의 양자회로에 적용한 함수합성 결과를 제시하였다. 끝으로 6장에서 결론을 논하였다.

II. 배경 이론

양자논리는 정보비트를 치수(radix)에 따라 다르게 부른다. 2-치(value) 양자정보 비트는 qubit(quantum binary bit), 3-치 양자정보 비트는 qutrit(quantum ternary bit), 그리고 일반적인 양자 다치-비트는 qudit(quantum multiple-valued bit)이라 부른다[1]. 본 논문에서는 표기의 간편성을 위해 Toffoli는 T, Fredkin은 F, NOT는 N, controlled-NOT는 cN, root-of-NOT은 V, Controlled-V는 cV, 그리고 control-U는 cU로 각각 표기하기로 한다. 가장 일반적인 양자게이트 연산은 n-qubit의 2n-차원 Hilbert 공간 $H^{\otimes n}$ 상의 $2^n \times 2^n$ 유니터리(unitary) 행렬 연산이다. $H^{\otimes n}$ 상의 개별 qubit들 간의 연산은

$$U^n = U^{(1)} \otimes U^{(2)} \otimes \cdots \otimes U^{(n)} \tag{1}$$

과 같은 텐서 연산을 갖기 때문에 일반적인 유니터리 변환을 생성할 수 없다. 따라서 최소한 두 개 이상의 qubit들에 대한 '자명하지 않은 해' (nontrivial) 연산의 수행이 요구되며, $H^{\otimes n}$ 상의 어떤 unitary 변환은 1-qubit에 대해 cN의 적(product)과 유니터리 변환으로 분해될 수 있다. cN 게이트의 4×4행렬 표현은 매우 유용하다. qubit들의 항에서 cN 연산은 다음 연산에 대응한다.

$$\begin{aligned} &|00> \rightarrow |00> \\ &|01> \rightarrow |01> \\ &|10> \rightarrow |11> \\ &|11> \rightarrow |10> \end{aligned} \tag{2}$$

$\{|00>, |1>, |10>, |11>\}$ 기저(basis)들에 대한 행렬 표현은 아래와 같다.

$$cNOT = \begin{bmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & \sigma_x \end{bmatrix} \tag{3}$$

$$U = \sqrt{\sigma_x} = \frac{1}{1+i}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \tag{4}$$

식(3)은 cN이 결코 텐서 적이 될 수 없음을 보여준다. $U = V$일 때 식(4)은 V-게이트라 부르며 V-게이트와 켤레(conjugate), 전치(transpose) 및 켤레전치(transpose conjugate) 관계에 있는 수반(adjoint) 게이

트들은 각각 V^*, V^T 및 $V^\dagger$로 표기 한다. cN 게이트의 일반화는 cU 게이트이다. cU 게이트는 x=0이면 타깃 비트를 통과시켜 보전하고, x=1이면 $|y>\rightarrow U|y>$ 같이 타깃 비트에 작용한다. cU 게이트 구성은 cN 게이트의 구성으로부터 시작할 수 있는데, 이때 행렬 σ_x는 식(5-3)과 같은 2×2 유니터리 행렬로 대치될 수 있다[1],[7-8].

$$cU \equiv \begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix} \tag{5}$$

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{6}$$

$$U^2 = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = N \tag{7}$$

$$CBA = I \tag{8}$$

따라서 식(8)을 만족하는 세 개의 유니터리 연산자 A, B 및 C가 요구된다. 식(7~8)을 결합하면 식(9)의

$$C\sigma_x B\sigma_x A = U \tag{9}$$

cN 연산자가 생성되며, 그 실현이 그림 1이다[7].

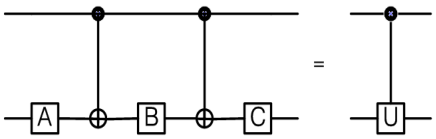

그림 1. cU 게이트의 구성
Fig. 1 A construction of cU gate

cU 게이트의 행렬 연산은 기저벡터들의 단순 순환(permutation)이다[1].

$$V|0> = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix} = |V_0> \tag{10}$$

$$V|1> = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1-i \\ 1+i \end{pmatrix} = |V_1> \tag{11}$$

$$V|V_0> = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0> \tag{12}$$

$$V|V_1> = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1-i \\ 1+i \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1> \tag{13}$$

$$N|0> = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1> \tag{14}$$

$$N|1> = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0> \tag{15}$$

P.1~P.3은 cU 게이트의 행렬연산 성질이다[1-8].

P.1 $N^2 = VV^\dagger = I$
P.2 $V^2 = (V^\dagger)^2 = N$
P.3 $V^* = V^\dagger$, $V = V^T$, $V^\dagger = V^{-1}$

고전적 알고리듬의 전치에 의해 함수 $f(x)$에 대한 양자논리 회로를 구하는 양자병렬처리에서 $f(x)$에 필요한 비트정보를 저장하기 위해 필요한 입출력 1-qubit 레지스터를 각각 x와 y라고 하면 연산자 U_f에 의한 양자 정보 x와 y의 정보처리 결과는 식(16)과 같다.

$$(x,y) \xrightarrow{U_f} (x, y \oplus f(x)) \tag{16}$$

식(16)에서 y=0라면

$$(x,0) \xrightarrow{U_f} (x, f(x)) \tag{17}$$

이때 U_f가 유니터리라면

$$(x,[y \oplus f(x)]) \xrightarrow{U_f} (x,[y \oplus f(x)] \oplus f(x)) = (x,y) \tag{18}$$

와 같이 $f(x) \oplus f(x) = 0$이므로 $U_f^2 = I$이다[1,7~8].

$$U_f|x \otimes 0> = |x \otimes f(x)> \tag{19}$$

$$U_f|x \otimes y> = |x \otimes [y \oplus f(x)]> \tag{20}$$

III. 양자회로의 함수 표현법 고찰

M.M.Rahman[2] 등이 사용한 양자함수 표현법은 6원소 양자 게이트 연산을 식(21)과 같이 표현하였다.

$$TQ = T(b)\,V^{+}(b,a)\,T(a,b)\,V(b,a)\,T(b)\,T(b,a) \quad (21)$$

식(21)에서 $T(b)$는 타깃 입력이 b임을 나타내며, $V^{+}(b,a)$는 제어 입력이 b이고 타깃입력이 a인 V^{+}게이트를 의미한다. $T(C,T)$는 제어 입력 C와 타깃입력 T를 갖는 T게이트를 의미한다. 이 함수 표현법은 컴퓨터 프로그램에 적합한 언어적 구조를 갖고 있는 반면 직관적 회로 해석 측면이 어려운 구조이다. D.M.Miller[3] 등은 M(C;t), T(a,b;t), CN(a:t)와 같은 표기법을 사용하여 T(a,b;t)와 같이 복수의 제어입력들을 모두 표기함으로써 정보의 구체성을 높였지만 이 방법은 M.M.Rahman[2] 방법과 유사한 함수표현 방법이다.

$$M(C;T) = V(a_0;t)M_0(C_0;a_0)\,V^{+}(a_0;t)M_1(C_1;a_0)\;V(a_0;t)M_2(C_0;a_0)\,V^{+}(a_0;t)M_3(C_1;a_0) \quad (22)$$

M.Socken[4] 등도 M.M.Rahman[2]과 D. M. Miller[3] 방법과 유사한 함수 표현 방법을 사용하였다. 예를 들면 제어입력 C와 타깃입력 x_i인 신호의 제곱연산이 항등임을

$$T(C,x_t)\,T(C,x_t) = I \quad (23)$$

과 같이 나타내었다. 이상의 방법들은 괄호와 콤마 등의 기호와 약어 문자에 함수 식별기능을 부여하여 양자회로의 함수를 서술적 문장으로 표현한 경우들로서 컴퓨터 입력에 적합한 문법구조를 갖는 함수 표현법들이라 할 수 있다. R.Wille[5] 등은 U게이트를

$$U^{G}(X,Y) = g_k(X), \text{if}\,[y_1 \cdots y_{\lceil \log q \rceil}]_2 < q \quad (24)$$

$$= X, otherwise$$

; $G=\{g_0,\cdots,g_{q-1}\}$, $q\in N$, N=게이트 수

; $X=\{x_1,\cdots,x_n\}$

; $Y=\{y_1,\cdots,y_{\lceil \log q \rceil}\}$

같이 정의한 후 함수를 식(25) 같이 표현하였다.

$$F_d = U^{G}(U^{G}(\cdots(U^{G}(F_0,Y_1),Y_2)\cdots,Y_{d-1}),Y_d) \quad (25)$$

이 방법은 입력 X_i과 2진 선택입력 Y_i에 대한 i번째 유니버설 게이트를 i+1번째 입력으로 $U^{G}(X_i, Y_i)=X_{i+1}$과 같이 정의함으로써 입출력 함수가 종속관계로 명확하고 2진 게이트 선택신호 집합 Y에 따라 게이트 U^{G}가 항등 또는 주어진 집합 G의 게이트로 작동한다. 이 방법은 게이트 간 입출력 정보와 U^{G} 게이트의 구체성 측면에서 앞의 방법들보다 구체적인 함수표현 방법이라 할 수 있지만 계산 방법이 복잡하여 컴퓨터 해석에 적합하다. M.Perkowski[1]가 사용한 식(26)의 함수표현법은 위의 방법들보다 표현된 함수가 수학적 구조에 가까워 이해가 쉬운 장점이 있으나 수식과 문장을 병행적으로 사용함으로써 불완전한 수학적 표현이다. 특히 식(26)에는 타깃양자 d의 연산이 포함되지 않아 추가적 연산과정이 요구됨을 알 수 있다.

$$[c\oplus \bar{a}b\oplus a\bar{b}\bar{c}]\,CONTROL\sqrt{NOT}\;\bullet$$
$$[b\oplus \bar{a}bc]\,CONTROL\sqrt{NOT} \quad (26)$$

이상과 같이 양자회로의 함수표현과 관련된 최근의 연구 방법들은 컴퓨터 프로그램 처리에 적합한 함수 표현 방식들을 채택하고 있거나 복잡한 함수 구조를 갖고 있어 새로운 설계와 합성을 위한 직관적 이해가 어려운 실정이다. 그러므로 이해와 표기가 용이하면서 다양한 함수 정보를 포함하여 직관적 이해와 가독성을 높일 수 있는 새로운 방식의 함수표현 방법이 요구된다.

IV. 새로운 양자함수 표현법

4.1. 멱승 제어함수를 갖는 cU 게이트

정의 1. U_f의 제어변수가 X일 때 $f(X)$는 연산자 U의 멱함수이다.

$$U_f(X) = U^{f(X)} \quad (27)$$

정리 1. U_f가 NCV-의사-제어 게이트라면

$U_f|XY>=|X>\otimes|Y\oplus f(X)>$에 대하여

$$U_f|XY>=|X>\otimes U^{f(X)}|Y> \tag{28}$$

(증명) $0\le i\le n$일 때 $f(X)$는 i개-직렬 적(serial- product)된 U^{a_i} 멱함수에 대하여 a_i가 상수이면 순환 산술(arithmetic) 합이며, a_i가 x와 $\overline{x}$ 같은 균형(balanced) 변수일 경우는 순환 modulo 2의 합이다. $U_f=cN$인 2-qubit 연산은 $f(X)$가 상수일 때 $0\le m$ 및 $0\le k\le 3$인 정수에 대해 P.1과 P.2를 만족하기 위한 조건 $f(X)=4m+k$은

$$N^{4m+k}|Y>=I|Y>=|Y\oplus 0> \quad ;k\in\{0,2\},$$
$$N^{4m+k}|Y>=N|Y>=|Y\oplus 1> \quad ;k\in\{1,3\}.$$

만일 $f(X)$가 module 2 성질을 만족하는 균형 변수로서 $x\in\{0,1\}$인 x와 $\overline{x}$인 경우에는 $N^x|Y>$와 $N^{\overline{x}}|Y>$에 대해

$$N^x|Y>=N^0|Y>=|Y\oplus 0>=|Y>, \tag{29}$$

$$N^x|Y>=N^1|Y>=|Y\oplus 1>=|\overline{Y}>, \tag{30}$$

$$N^{\overline{x}}|Y>=N^{\overline{0}}|Y>=|Y\oplus\overline{0}>=|\overline{Y}>, \tag{31}$$

$$N^{\overline{x}}|Y>=N^{\overline{1}}|Y>=|Y\oplus\overline{1}>=|Y>, \tag{32}$$

$$\therefore |X>\otimes N^{f(X)}|Y>=|X>\otimes|Y\oplus f(X)>.$$

$U_f=cV$(및 $cV^{\dagger}$)일 때의 2-qubit 연산은 V^{a_i}의 i-직렬 적을

$$\prod_{i=n}^{1}V^{a_i}=V^{a_n}V^{a_{n-1}}\cdots V^{a_2}V^{a_1}=V^{f(X)} \tag{33}$$

과 같이 나타내면 $\sum_{i=1}^{n}a_i=f(X)$이므로 멱함수의 산술연산을 만족한다. 아래의 2-qubit 연산에 대하여

$$|X>\otimes V^{f(X)}|Y>=|X>\otimes\prod_{i=n}^{1}V^{a_i}|Y> \tag{34}$$

a_i가 상수라면 $f(X)=4m+k$로 순환하며, 균형 변수라면 식(29~32)과 같은 modulo 2 연산이다.

1) $k=0$이면 $V^{f(X)}=I$,
$V^{f(X)}|Y>=I|Y>=|Y\oplus 0>$

2) $k=1$이면 $V^{f(X)}=V$,
$V^{f(X)}|Y>=V|Y>=|V_Y>$

3) $k=2$이면 $V^{f(X)}=N$,
$V^{f(X)}|Y>=N|Y>=|Y\oplus 1>$

4) $k=3$이면 $V^{f(X)}=VN=NV$,
$V^{f(X)}|Y>=NV|Y>=|V_Y\oplus 1>$
$=|V_{Y\oplus 1}>=VN|Y>$

따라서 $k=1$과 $k=3$일 때 항등과 반전 연산을 만족하며, $k=2$과 $k=4$의 경우는 V 또는 $V^{\dagger}$연산자와의 추가 연산을 통해 항등과 반전 성질을 유지할 수 있으므로

$$|X>\otimes V^{f(X)}|Y>=|X>\otimes|Y\oplus f(X)>$$
$$|X>\otimes U^{f(X)}|Y>=|X>\otimes|Y\oplus f(X)>$$
$$\therefore U_f|XY>=|X>\otimes U^{f(X)}|Y>.$$
$$Q.E.D.$$

그림 2는 정리 1의 양자게이트 구성도이다.

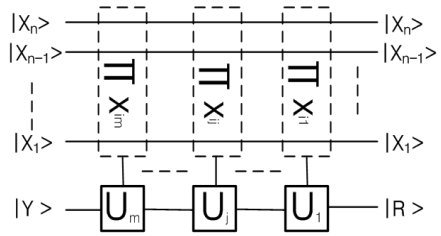

그림 2. 의사-제어된 NCV-게이트를 이용한 매크로 양자회로의 구성
Fig. 2 A construction of macro quantum circuit using affine-controlled NCV-gates

4.2. 의사-제어된 NCV-게이트 합성 알고리듬

의사-제어된 NCV-게이트들을 이용하여 정리 1과 그림 2를 만족하는 본 논문의 매크로 레벨 양자회로의 합성 알고리듬은 S.1~S.3의 3 단계로 구성된다.

S.1 제어입력 라인 상의 각 게이트 출력 노드에 제어입력 함수의 선형적 XOR 연산 결과인 함수

$f(X)$을 표기한다.

S.2 타깃 라인 상의 각 연산자 U_j에 직접적으로 작용하는 함수 $f(X)$을 구한 후 정리1에 의해 연산자 U_j의 멱함수로 표기한다.

S.3 연산자 U_j를 최 좌측에서 우측으로 j-직렬 적 배열한 후 타깃비트 $|Y>$와 적해 함수를 완성한다.

그림 3~4와 같이 의사-제어된 NCV-게이트들을 대상으로 본 논문의 함수합성법을 적용할 경우에 그림 3에 대한 본 논문의 합성 함수식은 아래와 같다.

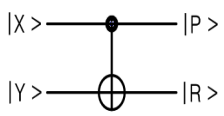

그림 3. cN 게이트
Fig. 3 cN 게이트

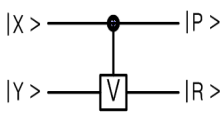

그림 4. cV 게이트
Fig. 4 cV 게이트

$$|R>=N^{X_1}|Y> \tag{35}$$

식(35)에서 $X=1$이면 $|R>=N|Y>=|1\oplus Y>$을 실행하고 $X=0$이면 $|R>=|Y>$을 실행하여 cN 게이트의 연산 성질을 만족함을 알 수 있다. 그림 4와 같은 cV(및 $cV^{\dagger}$)게이트 군에 대한 본 논문의 합성 함수식은 식(36)과 같다.

$$|R>=V^{X_1}|Y> \tag{36}$$

; $V=\frac{1}{2}\begin{pmatrix}1+i & 1-i\\ 1-i & 1+i\end{pmatrix}$, $V^{\dagger}=\frac{1}{2}\begin{pmatrix}1-i & 1+i\\ 1+i & 1-i\end{pmatrix}$.

이 경우도 $X=1$이면 $|R>=V|Y>=|V_Y>$을 실행하고, $X=0$이면, $|R>=|Y>$을 실행하여 cV 게이트 연산 성질을 만족함을 알 수 있다. cV 게이트의 수반 게이트인 $cV^{\dagger}$ 게이트의 경우도 동일한 결과를 얻을 수 있다.

Ⅴ. 매크로 레벨 양자회로의 함수 합성

5.1. 3-입력 T 게이트 함수의 합성 예

그림 5는 3-qubit T 게이트 회로로서 함수식은 식(37)의 $|R>=|X_2X_1\oplus Y>$와 같이 두 제어입력이 $X_2X_1=11$인 경우에 한해서 타깃 입력 Y에 대해 N 연산자로 작용한다. 그림 6은 그림 5에 대한 의사-제어된 NCV-게이트 실현이다[1-8].

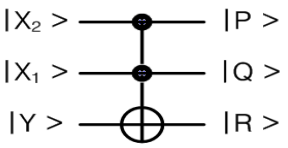

그림 5. 3-qubit T 게이트
Fig. 5 3-qubit T gate

$$|R>=|X_2X_1\oplus Y> \tag{37}$$

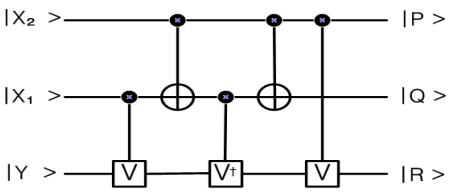

그림 6. 그림 5의 의사-제어된 게이트 실현
Fig. 6 A realization of fig.5 using affine-controlled NCV-gates

그림 6을 본 논문의 함수합성법으로 합성하면

$$|P>=|X_2> \tag{38}$$

$$|Q>=|X_1> \tag{39}$$

$$|R>=V_3^{X_1}V_2^{\dagger X_2\oplus X_1}V_1^{X_2}|Y> \tag{40}$$

과 같다. 식(37)과 식(40)에 대한 2-qubit 제어입력 인가시의 함수식 연산결과는 아래와 같다.

1) $|X_2X_1>=|00>$

$|R>=V_3^0V_2^{\dagger 0\oplus 0}V_1^0|Y>=|Y>$

$|X_2X_1 \oplus Y> = |0 \oplus Y> = |Y>$

2) $|X_2X_1> = |01>$

$|R> = V_3^1 V_2^{\dagger 0 \oplus 1} V_1^0 |Y> = V_3 V_2^{\dagger} |Y>$

$= I|Y> = |Y>$

$|X_2X_1 \oplus Y> = |0 \oplus Y> = |Y>$

3) $|X_2X_1> = |10>$

$|R> = V_3^0 V_2^{\dagger 1 \oplus 0} V_1^1 |Y> = V_2^{\dagger} V_1 |Y>$

$= I|Y> = |Y>$

$|X_2X_1 \oplus Y> = |0 \oplus Y> = |Y>$

4) $|X_2X_1> = |11>$

$|R> = V_3^1 V_2^{\dagger 1 \oplus 1} V_1^1 |Y> = V_3 V_1 |Y>$

$= V^2|Y \geqq N|Y> = |1 \oplus Y>$

$|X_2X_1 \oplus Y> = |1 \oplus Y>$

$\therefore |X_1X_2 \oplus Y> = V_3^{X_1} V_2^{\dagger X_2 \oplus X_1} V_1^{X_2} |Y>$

5.2. Distance-3 Hamming 코드 실현

그림 7의 예제는 distance=3인 Hamming 코드의 minterm들을 의사-제어 게이트로 실현한 것이다[1].

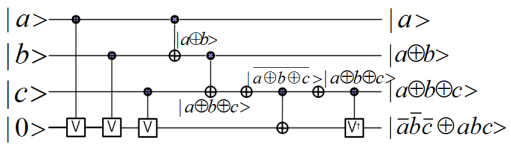

그림 7. 의사-제어된 NCV- 게이트들에 의한 Hamming-distance-3 minterm 실현

Fig. 7 A realization of Hamming-distance-3 minterms using affine-controlled NCV-gates

그림 7의 타깃출력

$$|R> = \bar{a}\bar{b}\bar{c} \oplus abc \tag{41}$$

에 대한 본 논문 방법의 함수합성은 식(42)이다.

$$|R> = V^a V^b V^c N^{\overline{a \oplus b \oplus c}} V^{\dagger a \oplus b \oplus c} |0> \tag{42}$$

식(41~42)에 대해 각각 3-qubit 제어변수를 입력시켰을 경우의 연산결과는 동일한 결과를 보여 준다.

1) $|abc> = |000>$

$|R> = V^0 V^0 V^0 N^{\overline{0 \oplus 0 \oplus 0}} V^{\dagger 0 \oplus 0 \oplus 0} |0>$

$= N|0> = |1>$

$|\bar{a}\bar{b}\bar{c} \oplus abc> = |1 \oplus 0> = |1>$

2) $|abc> \in \{|001>, |010>, |100>\}$

(1) $|R> = |001>$인 경우

$|R> = V^0 V^0 V^1 N^{\overline{0 \oplus 0 \oplus 1}} V^{\dagger 0 \oplus 0 \oplus 1} |0>$

$= VV^{\dagger}|0> = I|0> = |0>$

$|\bar{a}\bar{b}\bar{c} \oplus abc> = |0 \oplus 0> = |0>$

(2) $|abc> \in \{|010>, |100>\}$ 동일

3) $|abc> \in \{|011>, |101>, |110>\}$

(1) $|R> = |011>$인 경우

$|R> = V^0 V^1 V^1 N^{\overline{0 \oplus 1 \oplus 1}} V^{\dagger 0 \oplus 1 \oplus 1} |0>$

$= V^2 N|0> = N^2|0> = |0>$

$|\bar{a}\bar{b}\bar{c} \oplus abc> = |0 \oplus 0> = |0>$

(2) $|abc> \in \{|101>, |110>\}$ 동일

4) $|abc> = |111>$

$|R> = V^1 V^1 V^1 N^{\overline{1 \oplus 1 \oplus 1}} V^{\dagger 1 \oplus 1 \oplus 1} |0>$

$= V^3 N^0 V^{\dagger}|0> = V^2 VV^{\dagger}|0> = |1>$

$|\bar{a}\bar{b}\bar{c} \oplus abc> = |0 \oplus 1> = |1>$

$\therefore |R> = |\bar{a}\bar{b}\bar{c} \oplus abc>$

한편 Perkowski[1]의 함수 표현식인 식(26)을 본 논문 방법으로 표현하면 다음과 같다.

$$R = V^{c \oplus \bar{a}b \oplus a\bar{b}\bar{c}} V^{b \oplus \bar{a}bc} |d> \tag{43}$$

이상과 같이 임의 매크로 양자회로를 의사-제어된 NCV-게이트들을 이용하여 실현하기 위한 본 논문의 함수합성 알고리듬은 본 논문 방법으로 합성된 함수들이 타깃입력 함수와 제어입력 함수에 대한 구체적 함수 정보를 포함하고 있음을 보였다. 또한 본 논문의 제안 알고리듬은 의사-제어된 NCV-게이트들이 U_f 연산자로서의 고유한 유니터리 연산 성질을 만족시킬 수 있는 방법임을 확인할 수 있었다.

Ⅵ. 결 론

논문에서는 양자회로 합성을 위한 새로운 함수표현법을 제안하였다. 본 논문 방법은 합성된 함수 구조가 기존 방법들처럼 서술적 표현구조가 아닌 수식적 표현구조를 가지며, 함수식에 입출력 타깃 정보와 제어함수 정보 및 유니터리 연산자 정보를 포함하고 있어 양자회로 이해를 위한 직관적 사고와 이해를 가능하게 해 준다. 특히 유니터리 연산자의 제어함수를 대응하는 연산자의 멱함수로 표현하는 수학적 치환을 통해 타깃라인 상에서 직렬적 된 유니터리 연산자들의 스칼라 연산이 멱함수에 의한 산술 연산과 modulo 2 연산으로 실행될 수 있게 함으로써 수학적 구조가 간단하고 함수 이해가 용이한 새로운 함수합성 방법을 개발할 수 있었다. 향후 연구과제는 본 논문의 함수합성법을 이용해 고전적 논리 회로들을 매크로 게이트를 통하지 않고 의사-제어된 NCV-게이트들로 직접 실현하는 함수합성법의 개발이다.

참고 문헌

[1] M. Perkowski. *Quantum Robotics*. Springer Verlag, 2012.

[2] M. M. Rahman, A. Baberjee, G. W. Dueck, and A. Pathak, "Two-Qubit Quantum Gates to Reduce the Quantum Cost of Reversible Circuit," *IEEE 41th Int. Symp. on Multiple-Valued Logic*, 2011. p. 86-92.

[3] D. M. Miller, R. Wille, and Z.Sasanian, " Elementary Quantum Gate Realization for Multiple-Control Toffoli Gtaes," *IEEE 41th Int. Symp. on Multiple-Valued Logic*, 2011, pp. 288-293.

[4] M. Socken, Z. Sasanian, R. Wille, D. M. Miller, and R. Drechsler, "Optimizing the Mapping of Reversible Circuits to Four-Valued Quantum Gate Circuits," *IEEE 42th Int. Symp. on Multiple-Valued Logic*, 2012, pp. 173-178.

[5] R. Wille, H. M. Le, G. W. Deuck, and D.Große, "Quantified Synthesis of Reversible Logic," *Proceedings of the conference on Design, automation and test in Europe*, 2008. pp. 1015-1020.

[6] A. D. Vos and S. D. Baerdemacker, "The roots of the NOT gate," *IEEE 42th Int. Symp. on Multiple-Valued Logic,* 2012, pp. 167-172.

[7] M. L. Bellac. *A Short Introduction to Quantum Information and Quantum Computing*. Cambridge University Press, 2006.

[8] D. Ahn. *Technology Trends and Market Forecasts of Quantum Information Communications*. Ha Yeon, Oct. 15, 2012.

저자 소개

박동영(Dong-Young Park)

1980년 인하대학교 전자공학과 졸업(공학사)
1985년 인하대학교 대학원 전자공학과 졸업(공학석사)
1995년 인하대학교 대학원 전자공학과 졸업(공학박사)
2014년 강릉원주대학교 정보통신공학과 교수
※ 관심분야 : 다치논리 회로, 양자정보통신, 가역회로 설계

정연만(Yeon-Man Jeong)

1983년 숭실대학교 전자공학과 졸업(공학사)
1985년 숭실대학교 대학원 전자공학과 졸업(공학석사)
1991년 숭실대학교 대학원 전자공학과 졸업(공학박사)
2014년 강릉원주대학교 정보통신공학과 교수
※ 관심분야 : 통신신호처리, 무선통신시스템, RF IC 설계