International Journal of Scientific & Engineering Research, Volume 6, Issue 5, May-2015 1477
ISSN 2229-5518

Indexed formalized operators for n-bit circuits

Nikolay Raychev

Abstract - in this report is considered the construction of *n* qubit circuits through the addition of *n* qubits as a quantum register, at which each bit is a set index in a range from 0 to *n* - 1. The index of the bit complies with its significance within the space of the classical state. An indexed formalized operator is presented, that extends the single qubit operator to a *n* qubit operator, that acts to an individual qubit.

Index Terms— boolen function, circuit, composition, encoding, gate, phase, quantum.

---

1 INTRODUCTION

In this report is examined the construction of indexed qubit operators, which include more than one control or target bit, based on a formalized qubit operator. This work is part of the developed from the author formalized system for design of algorithmic models for quantum circuits, based on phase encoding, decoding and parameterization of primitive quantum operators. In previous publications of the author [6, 7, 8] were defined several sets of operators on the n qubit, which generalize certain classical characteristics: identity and logical negation. When n qubit circuits are considered, usually it is a matter of addition of n qubits as a quantum register, in which at each bit is given an index in a range from 0 to n – 1. The index of the bit complies with its significance within the space of the classical state. Therefore the i-th bit corresponds to the bit, located in position 2^i of a n bit string. In this publication the formalized single qubit operator is used to construct basic, elementary building blocks of n qubit circuits: single qubit operators in the n qubit state and two qubit controlled operators. The report presents the indexed, formalized operator. These operators extend the single qubit operator to a n qubit operator, which acts on an individual qubit.

2 INDEXED SINGLE QUBIT OPERATORS

It is possible to extend the formulas for single qubit space to the n qubit space by adding an index parameter t. The index parameter directly corresponds to the index of the qubit to which the operator will be applied. When A is a single qubit, formalized operator, then $A_{[t]}$, the indexed form of that operator, designates that A is applied to qubit t. If x is an n qubit basis state and $0 \leq t \leq n-1$. Then the application of an indexed, formalized gate to a basis state $|x\rangle$ is,

$$U_{[t]}(a,\gamma\iota\eta)|x\rangle = (-1)^{\varepsilon'(\gamma\iota\eta)_0(x_t)}\sqrt{a}|x\rangle + (-1)^{\varepsilon'(\gamma\iota\eta)_1(x_t)}\sqrt{1-a}\,|x \oplus 2^t\rangle \qquad (1)$$

It should be noted that the phase encoding is only relative to the value of bit t and the negation of $|x\rangle$ is not the logical negation of x, but the state in which bit t is with a negative value. The value 2^t is assumed to be an n bit representation of 2^t, such that $x\oplus 2^t$ reverse only bit t in x and leaves all other bits unchanged.

When determining the probability amplitude $\langle y|U_{[t]}|x\rangle$ must be taken into account the difference of the t-th bit in x and y. If they are the same, the phase function $\mathcal{E}_0$ is used and the amplitude is $\sqrt{\alpha}$. In case that they are different, the phase function $\mathcal{E}_1$ is used and the amplitude is $\sqrt{1-\alpha}$, This may be captured in a general equation for $\langle y|U_{[t]}|x\rangle$.

$$\langle y|U_{[t]}|x\rangle(\alpha, \quad \gamma\iota\eta)|x\rangle = \begin{cases} (-1)^{\varepsilon'(\gamma\iota\eta)_{x_i\oplus y_t}x_t}\,{}^{x_i\oplus y_t}\sqrt{a}\,{}^{-x_i\oplus y_t}\sqrt{1-1} & y \in \{x, x\oplus 2^t\} \\ 0 & otherwise \\ (-1)^{\varepsilon(\gamma\iota\eta)_0(x_t)}\sqrt{a} & y = x \\ (-1)^{\varepsilon(\gamma\iota\eta)_1(x_t)}\sqrt{a} & x = x\oplus 2^t \\ 0 & y \notin \{x, x\oplus 2^t\} \end{cases} \qquad (2)$$

The formalized single qubit operator is a linear combination of an identity operator and a negation operator. However, this is not true for their indexed forms. For example, if $A = U(a,\gamma\iota\eta) = \sqrt{a}\,\mathfrak{I}_{\gamma\iota} + \sqrt{1-a}\,\mathcal{N}_{\gamma\eta}$ is a formalized operator, then its indexed form $A_{[t]}$ has the following decomposition,

$$A_{[t]} = I^{\otimes(2^n-t-1)} \otimes A \otimes I^{\otimes t}$$
$$= \sqrt{a}\left(I^{\otimes(2^n-t-1)} \otimes \mathfrak{I}_{\gamma\iota} \otimes I^{\otimes t}\right)$$
$$= \sqrt{1-a}\,(I^{\otimes(2^n-t-1)} \otimes \mathcal{N}_{\gamma\eta} \otimes I^{\otimes t}) \qquad (3)$$

While the operator $\left(I^{\otimes(2^n-t-1)} \otimes \mathfrak{I}_{\gamma\iota} \otimes I^{\otimes t}\right)$ is obviously in Ext_n, the operator $(I^{\otimes(2^n-t-1)} \otimes \mathcal{N}_{\gamma\eta} \otimes I^{\otimes t})$ is not in the set of the n qubit negation operators $N\mathrm{ext}_n$. On the other hand, it is an operator, which connects basis x with some other basis y, where $x \neq y$. Such an operator can be represented by a signed permutation matrix which connects {0, 1, … , 2^n-1} to a permutation $\sigma = \{\sigma(0), \sigma(1), \dots, \sigma(2^n-1)\}$ such that $\sigma(i) \in \{0, 1, \dots, 2^n-1\}$ and $\sigma(i) \neq i$. Now a system can be developed that captures both single qubit operators and their indexed forms. Then the operator parameters determine where the indexed
operators fit within the system. It can be started with a set of n bit basis operators that
do not identify basis states.

Definition 1.1 Υ_n *is the set of the n qubit operators where for each* $c, b \in \mathbb{B}^n$ *with* $c \neq b$ *and* $V \in \Upsilon_n$

$V|b\rangle = \pm|c\rangle$

The operators in the set Υ_n *can be represented by a* $2^n x 2^n$ *signed permutation matrices where for each* $v \in \Upsilon_n$ *there exists a permutation* σ *of* $\{0, 1, \ldots, 2^n\text{-}1\}$, such that $v_{\sigma(i)i} = \pm 1$, and there does not exists an *i, for which* $\sigma(i) = i$.

Conditionally will be assumed, that column i, unlike line i encodes $\sigma(i)$, such that

$$v|x\rangle = \pm|\sigma(x)\rangle \tag{4}$$

As was noticed at the single qubit basis operators, each basis operator effectively encodes a boolean function. This extends to n qubit basis operators and through Theorem 3.1, it is possible to be developed a unified system for operation with phase encoding functions of a single bit operator, whether they're indexed or not. First, let's note that the set Ext_n encodes the set of the n bit boolean functions $\mathcal{B}^n$.

Theorem 1.1 Ext_n *and* $\mathcal{B}^n$ *are isomorphic.*

Proof. If $f \in \mathcal{B}^n$ is an n bit boolean function. Then $A \in \text{Ext}_n$, defined by

$$A_{ij} = (-1)^{f(i)}\delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j \text{ and } f(i) = 0 \\ -1 & i = j \text{ and } f(i) = 1 \end{cases} \tag{5}$$

The bijection follows from the construction of A.

In this way can be described the action of $A \in \text{Ext}_n$, applied to the n qubit basis $|x\rangle$ in respect of the boolean function f, encoded by A.

$$A|x\rangle = (-1)^{f(x)}|x\rangle \tag{6}$$

The function *Id, given in* equation 4.4 can be used to map boolean functions to operators in Ext_n. The n bit boolean function can be enumerated based on the binary representation of $i \in \{0, 1, \ldots, 2^n - 1\}$, where $f \in \mathcal{B}^n$ is defined as $f(i) = 0$, if bit i of k is 0, and $f(i) = 1$, if bit i of k is 1. All operators in Υ_n can be decomposed into the product of an operator in Ext_n and an unsigned permutation matrix such that the phase encoding carried out by the operator is separated from the basis change encoded in the permutation.

Theorem 1.2 *If operator* $v \in \Upsilon_n$ *is a signed permutation operator which for all basis* $|x\rangle$ *encodes phase function f on to the permutation* σ *as follows,*

$$v|x\rangle = (-1)^{f(x)}|\sigma(x)\rangle \tag{7}$$

Then there exists the permutation matrix B and the operators $F, G \in \text{Ext}_n$*, which encode* σ *and the boolean functions f and g, respectively with* $g = f^\circ\sigma^{-1}$*, such that* $v = B^\circ ID_f = ID_g{}^\circ B$*. More over,* $f = ID_f$ *and* $g = ID_g$*.*

Proof. For a given v, the operators *F, G and B* can be constructed as follows.

$$F_{ij} = (-1)^{f(i)}\delta_{ij} \qquad G_{ij} = (-1)^{g(i)}\delta_{ij} = (-1)^{f(\sigma^{-1}(i))}\delta_{ij}$$

where $(-1)^{f(i)}$ is the non-zero value in column i of v, and $(-1)^{f(\sigma^{-1}(i))}$ is the non-zero value in column i of $v^\dagger$, or alternative row i of v. For operator *B:* $B_{ij} = |v_{ij}|$ for all $i, j \in \{0, 1, \ldots, 2^n\}$. It then follows that for each $x \in \mathbb{B}^n$

$$BF|x\rangle = (-1)^{f(x)}B|x\rangle = (-1)^{f(x)}|\sigma(x)\rangle$$

$$GB|x\rangle = C|\sigma(x)\rangle = (-1)^{f(\sigma^{-1}(\sigma(x)))}|\sigma(x)\rangle = (-1)^{f(x)}|\sigma(x)\rangle$$

Now the indexed operators can be expressed as a linear combination of an identity operator and a negation operator Υ_n.

Theorem 1.3 *if operator* $V = U_{[t]}(\alpha, \gamma\iota\eta)$ *is formalized, indexed n qubit operator. In such case there are* $A \in \text{Ext}_n$ *and* $B \in \Upsilon_n$*, such that*

$$V = \sqrt{\alpha}A + \sqrt{1-\alpha}B \tag{8}$$

Proof. The operator A is defined as

$$A = \sum_{i=0}^{2^n-1}(-1)^{\varepsilon(\gamma\iota\eta)_0(i_t)}\,|i\rangle\langle i| \tag{9}$$

Obviously the operator A is in Ext_n.

The operator B is defined as

$$B_{xy} = \begin{cases}(-1)^{\varepsilon(\gamma\iota\eta)_1(i_t)} & x = y \oplus 2^t \\ 0 & otherwise\end{cases} \tag{10}$$

Obviously the operator B is in Υ_n.

From equation 1 is obtained the following decomposition of V

$$V = \left(I^{\otimes(n-t-1)} \otimes U(a, \gamma\iota\eta) \otimes I^{\otimes t}\right)$$
$$= I^{\otimes(n-t-1)} \otimes (\sqrt{a}\,\mathfrak{I}_{\gamma\iota} + \sqrt{1-a}\mathcal{N}_{\gamma\eta}) \otimes I^{\otimes t})$$
$$= \sqrt{a}\,(I^{\otimes(n-t-1)} \otimes \mathfrak{I}_{\gamma\iota} \otimes I^{\otimes t}) + \sqrt{1-a}(I^{\otimes(n-t-1)} \otimes \mathcal{N}_{\gamma\eta} \otimes I^{\otimes t})$$

The operator: $I^{\otimes(n-t-1)} \otimes \mathcal{N}_{\gamma\eta} \otimes I^{\otimes t}$ свързва $|x\rangle$ с $(-1)^{\varepsilon(\gamma\iota\eta)_1(x_t)}|x \oplus 2^t\rangle$ for each x. In matrix form this corresponds to $(-1)^{\varepsilon(\gamma\iota\eta)_1(x_t)}$ at row $x \oplus 2^t$ and column x and is exactly operator *B.*

The operator $I^{\otimes(n-t-1)} \otimes \mathfrak{I}_{\gamma\iota} \otimes I^{\otimes t}$ свързва $|x\rangle$ с $(-1)^{\varepsilon(\gamma\iota\eta)_0(x_t)}|x\rangle$ for each x, and is exactly operator A. If it is given that $N\text{ext}_1 \equiv \Upsilon_1$, this form captures both the single qubit operators and their indexed forms. As a corollary to Theorem 1.3 is provided the characterization of the matrix representation of an elementary indexed operator.

Corollary 1.4 *If* $A = U_{[t]}(\alpha, p_A)$*, then the matrix form of A is defined such that,*

$$A_{ij} = \begin{cases} (-1)^{\mathcal{E}(p_A)_0(i_t)}\sqrt{\alpha} & i = j \\ (-1)^{\mathcal{E}(p_A)_1(i_t)}\sqrt{1-\alpha} & i = x \oplus 2^t \\ 0 & \text{otherwise} \end{cases} \quad (11)$$

Proof. By Theorem 1.3 it is known that when $j = i$, the amplitude is $\sqrt{\alpha}$, when $j = \sigma(i) = i \oplus 2^t$ – it is $\sqrt{1-\alpha}$, and in all other cases the amplitude is zero. Finally, from equations 1 and 2 it is visible, that the phase function on the main diagonal is $\mathcal{E}(p_A)_0(i_t)$ with the other non-zero entries having $\mathcal{E}(p_A)_1(i_t)$.

Phase Encoding and Decoding

From equation 3.2 and Theorem 1.3 can be determined the encoding pattern of an indexed operator. When considering some fixed target bit *t*, operator $A_{[t]}$ is decoded by the indexed form of the same operators that decode A.

Theorem 1.5 *if A and B are formalized operators, such that B is a decoder of A and BA = C for some* $C \in \mathrm{Ext}_1 \cup N\mathrm{ext}_1$. *Then, for each* $t \in \{0, 1, \ldots, n\text{-}1\}$, $B_{[t]}A_{[t]} = C_{[t]}$.

Proof. The proof follows from equation 3.2.

Since, it is a rare case that are concerned operators applied to a fixed target bit *t*, therefore, must be given some consideration to the interaction between operators that have different target bits.

As seen in Theorem 1.3, the structure of an indexed operator is characterized by the linear combination of an identifier from Ext_n and a "not" operator from Υ_n.. The latter of these operators can in turn be decomposed into the product of an operator from Ext_n, which encodes the phase changes of the operator, and a permutation operator, which encodes the basis changes. By understanding the composition of these *n* qubit basis operators, the composition of the linear combinations of these operators can be evaluated more easily.

Theorem 1.6 *If I(f) designates an operator in* Ext_n, *which encodes the phase function f, and N(σ, g)* designates an operator in Υ_n, *which encodes the phase function g in the permutation σ. Then*

$$I(f)I(g) = I(f \oplus g)$$

$$\mathrm{N}(\sigma, \mathrm{g})\mathrm{I}(\mathrm{f}) = \mathrm{N}(\sigma, \mathrm{f} \oplus \mathrm{g})$$

$$I(f)\mathrm{N}(\sigma, \mathrm{g}) = N(\sigma, (\mathrm{f} \circ \sigma^{-1}) \oplus \mathrm{g})$$

$$N(\sigma_a, f)N(\sigma_b, g) = N(\sigma_a \circ \sigma_b, (\mathrm{f} \circ \sigma_b) \oplus \mathrm{g})$$

(12)

Proof. The first case is a result from the multiplication of the matrix representations of *I*(*f*) and *I*(*g*). If $A = I(g)$ and $B = I(f)$ such that $A_{ij} = (-1)^{g(i)}\delta_{ij}$ and $B_{ij} = (-1)^{g(i)}\delta_{ij}$. From here follows, that $(BA)_{ij} = (-1)^{f(i)}(-1)^{g(j)}\delta_{ij} = (-1)^{g(j)\oplus f(i)}\delta_{ij}$ the Remaining equations follow from the first equation and theorem 3.1.2.

When dealing exclusively with indexed, formalized operators it is necessary only to be considered a special case of Theorem 1.6 in which the phase and permutation functions take on a specific form. The phase function of an indexed operator is always a member of $\mathcal{B}^1$, applied to the target bit. The permutation function simply maps a binary string *x* to the string where the target bit is reversed, $x \oplus 2^t$.

Theorem 1.7 *If the operators* $A = U_{[t_A]}(\alpha_A, (\gamma\iota\eta)_A)$ *and* $B = U_{[t_B]}(\alpha_B, (\gamma\iota\eta)_B)$ *are defined such that* $t_A \neq t_B$. *Then*

$$AB|x\rangle = (-1)^{\varepsilon((\gamma\iota\eta)_A)_0(x_{t_A}) \oplus \varepsilon((\gamma\iota\eta)_B)_0(x_{t_B})}\sqrt{a_A a_B} +$$
$$(-1)^{\varepsilon((\gamma\iota\eta)_A)_0(x_{t_A}) \oplus \varepsilon((\gamma\iota\eta)_B)_1(x_{t_B})}\sqrt{a_A(1-a_B)}|x \oplus 2^{t_B} +$$
$$(-1)^{\varepsilon((\gamma\iota\eta)_A)_1(x_{t_A}) \oplus \varepsilon((\gamma\iota\eta)_B)_0(x_{t_B})}\sqrt{(1-a_A)a_B}|x \oplus 2^{t_A} +$$
$$(-1)^{\varepsilon((\gamma\iota\eta)_A)_1(x_{t_A}) \oplus \varepsilon((\gamma\iota\eta)_B)_1(x_{t_B})}\sqrt{(1-a_A)(1-a_B)}|x \oplus 2^{t_B} \oplus 2^{t_A}$$

(13)

Proof. The operators *A and B* can be rewritten in the style of Theorem 1.6, as follows

$$A = \sqrt{a_A} I\varepsilon((\gamma\iota\eta)_A)_0(x_{t_A}) + \sqrt{1-a_A} N\left(x \oplus 2^{t_A}, \varepsilon((\gamma\iota\eta)_A)_1(x_{t_A})\right)$$

$$B = \sqrt{a_B} I\varepsilon((\gamma\iota\eta)_B)_0(x_{t_B}) + \sqrt{1-a_B} N\left(x \oplus 2^{t_B}, \varepsilon((\gamma\iota\eta)_B)_1(x_{t_B})\right)$$

(14)

Given that $t_A \neq t_B$, then it follows that the permutations performed by both *A* and *B* do not effect the result of the opposing operator's phase functions as the targeted bits of the permutation, carried out by one of the operators, are not the target bits of the phase function of the other one. In such a case follows equation 13. Illustrated by corollary 1.7 is that encoding carried out by two or more indexed operators, none of which targets the same qubit, is not an expression of a function in $\mathcal{B}^1$, but the expression of a function in $\mathcal{B}^n$. Furthermore, when *A* and *B* have amplitudes in (0, 1), it is clear that *A* can not be a decoder of *B* in the sense of $AB|x\rangle \in \{\pm|x\rangle. \pm|x \oplus 2^{t_B}\rangle\}$. Therefore, an attention must be paid instead of the circumstances in which the operators targeting the same qubit can decode, but to the presence of indexed operators targeting other qubits. One important feature of the indexed operators, targeting different qubits, is that they change.

Theorem 1.8 *If* $A = U_{[t]}(\alpha_A, p_A)$ *and* $B = U_{[s]}(\alpha_B, p_B)$. *If s, t* $\in \{0, 1, \ldots, n-1\}$ *are such that* $s \neq t$, *then AB = BA.*

Proof. If *AB = BA*, then the commutator [*A, B*] = *AB – BA* is a zero matrix. From corollary 1.7 can be determined the matrix of *AB* and *BA*.

$$(AB)_{i,j} = \begin{cases} (-1)^{\varepsilon((\gamma\iota\eta)_A)_0(i)_i \oplus \varepsilon((\gamma\iota\eta)_B)_0(i_x)}\sqrt{a_A a_B} & j = i \\ (-1)^{\varepsilon((\gamma\iota\eta)_A)_0(i)_i \oplus \varepsilon((\gamma\iota\eta)_B)_1(i_x)}\sqrt{a_A(1-a_B)} & j = i \oplus 2^s \\ (-1)^{\varepsilon((\gamma\iota\eta)_A)_1(i)_i \oplus \varepsilon((\gamma\iota\eta)_B)_0(i_x)}\sqrt{(1-a_A)a_B} & j = i \oplus 2^t \\ (-1)^{\varepsilon((\gamma\iota\eta)_A)_1(i)_i \oplus \varepsilon((\gamma\iota\eta)_B)_1(i_x)}\sqrt{(1-a_A)(1-a_B)} & j = i \oplus 2^s \oplus 2^t \end{cases} \quad (15)$$

ISSN 2229-5518

The matrix of BA is that of AB, as shown in equation 15, but with all occurrences of A reversed with B and vice versa. In this way it can be found that $(AB)_{i,j} = (BA)_{i,j}$ and, therefore, *AB, BA = 0.*

Given that the indexed operators change, often a sequence of the indexed operators is rearranged, such that to be evaluated the decoding results with the decoder, applied immediately after the encoder. More specifically, let $\mathcal{U}$ be a sequence of indexed operators such that no two operators in $\mathcal{U}$ target the same qubit and $A_{[t]} \in \mathcal{U}$. If $\mathcal{U}' = \mathcal{U}\backslash\{A_{[t]}\}$ is the sequence without $A_{[t]}$, then $\mathcal{U} = A_{[t]}\mathcal{U}'$. Thus, if B is a decoder of A, then it is good to be examined the result of the sequence $B_{[t]}A_{[t]}\mathcal{U}'$.

Corollary 1.9 *If* $\mathcal{U} = A_k{}^\circ A_{k-1}{}^\circ \dots {}^\circ A_0$, *where* A_i *i is an indexed, formalized operator and for each* $i, j \in [0, k]$ *with* $i \neq j$, *then* A_i *and* A_j *do not target the same qubit. If* $B_{[t]}$ *is defined such that there exists some* A_i *in* $\mathcal{U}$, *which targets t, and* $B_{[t]}{}^\circ A_i = C_{[t]}$ *for* $C \in N\mathrm{ext}_1 \cup \mathrm{Ext}_1$ *(i.e. B decodes non-indexed* A_i*), then*

$B_{[t]}\mathcal{U} = C_{[t]}\mathcal{U}'$,
where $\mathcal{U}'$ *is* $\mathcal{U}$ *without* A_i.

Proof. From Theorem 1.8 it is known that $\mathcal{U}$ can be re-written as $A_i\mathcal{U}'$, and from Theorem 1.5 – that $B_{[t]}A_i\mathcal{U}' = C_{[t]}\mathcal{U}'$.

3 Conclusion

This research examines parallel arrays of indexed operators. Theorem 1 provides a means for constructing a summary encoding function of a parallel array of formalized operators, as well as general amplitudes for each basis state. This basic system for the parallel application of primitive operators was then used to address the specific case of applying an array comprised of a single operator to a register of qubits, a common occurrence in many quantum algorithms. The aggregate amplitude parameters for such an operator can be computed via corollary 1 and the reduced forms of the aggregated encoding functions are given in equation 8.8.

REFERENCES

[1] Barenco, A. A universal two-bit gate for quantum computation. Proceedings of the Royal Society of London A449 (1995), 679–683.
[2] Barenco, A., Bennett, C. H., Cleve, R., DiVincenzo, D. P., Margolus, N. H., Shor, P. W., Sleator, T., Smolin, J. A., and Weinfurter, H. Elementary gates for quantum computation. Physical Review A 52, 5 (1995), 3457–3467.
[3] Bernstein, E., and Vazirani, U. Quantum complexity theory. In Proceedings of the twenty-fifth annual ACM symposium on Theory of computing (New York, NY, USA, 1993), STOC '93, ACM, pp. 11–20.
[4] Bernstein, E., and Vazirani, U. Quantum complexity theory. SIAM J. Com- put. 26, 5 (1997), 1411–1473.
[5] Nikolay Raychev. Classical simulation of quantum algorithms. In International jubilee congress (TU), 2012.
[6] Nikolay Raychev. Unitary combinations of formalized classes in qubit space. In International Journal of Scientific and Engineering Research 04/2015; 6(4):395-398. DOI: 10.14299/ijser.2015.04.003, 2015.
[7] Nikolay Raychev. Functional composition of quantum functions. In International Journal of Scientific and Engineering Research 04/2015; 6(4):413-415. DOI:10.14299/ijser.2015.04.004, 2015.
[8] Nikolay Raychev. Logical sets of quantum operators. In International Journal of Scientific and Engineering Research 04/2015; 6(4):391-394. DOI:10.14299/ijser.2015.04.002, 2015.