Controlled formalized operators

Nikolay Raychev

Abstract - In this report is considered the generalization of the principles, which manage the formalization of controlled qubit operators. The research builds on the standard external data sources, for development of a generalized system for conditional operators. Certain controlled operators are viewed as linear combinations of universal operators. This system provides a generalized scheme for the type of the controlled operators, which could be encountered in a circuit, composed entirely of elementary operators.

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

1 Introduction

In this report is presented a formalized generalization of single qubit and controlled operators, based on formalized single qubit operator. This work is part of the developed by the author formalized system for designing 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. Moreover, some ways were explored in which can be constructed operators as linear combinations of elements from those sets. Such combinations capture the partial application of an operator together with another operator, which in a broader sense is its logical negation.

2 Controlled operators

The controlled operators conditionally use one of two single qubit operators. At the quantum computations is more appropriate to think that the condition for application is a condition on basis states, and not on the overall state. One approach for operation with controlled operators is to seek their basic definition and express their effect on basis states in terms of indexed formalized gates.

$$\langle y|CU_{[c][t]}(A,B)|x\rangle = \begin{cases}\langle y|A_{[t]}|x\rangle & x_c = 0\\ \langle y|B_{[t]}|x\rangle & x_c = 1\end{cases} \qquad (1)$$

The index c determines the control bit, while t specifies the target. Thus, the operator $A_{[t]}$ is applied when the c-th bit of x is 0, and $B_{[t]}$ – when it's 1. Viewed from the phase encoding/decoding perspective, the action of a controlled operator is to encode/decode with A to the subset of basis states x, where x_c = 0, and with B, where x_c = 1. While this approach to elementary controlled operators is elementary, the formalized system for designing of algorithmic models for quantum circuits offers a second approach, which unifies the elementary controlled operations with another important aspect of many quantum algorithms, the Oracle operators.

A standard technique in the design of quantum algorithms is the use of an Oracle operator to enact a phase-kickback operation [34]. Here an arbitrary, possibly irreversible function $f: \mathbb{B}^m \to \mathbb{B}^l$ is encoded into an $n = m + l$ qubit operator U_f, such that $U_f|xy\rangle = |x(y \oplus f(x))\rangle$, where $x \in \mathbb{B}^m$*, and* $y \in \mathbb{B}^l$. Normally are used higher degree bits for x and with a lower degree for y. The same could be carried out in reverse where $U_f|yx\rangle = |(y \oplus f(x)x)\rangle$. In both cases U_f acts as Oracle for f. Such operations are accepted as the controlled application of l qubit operator $\widehat{U_f}$, where x acts as control bit, and y as target. The phase kick-back occurs when the target qubits are set to an own state $\widehat{U_f}$, and the value of $f(x)$ is encoded into the phase of the resultant state. It is possible to apply this conception for the controlled operations to an elementary, two qubit controlled operators, which will provide a new means for viewing the behavior of the elementary controlled operations and the interference patterns that they generate.

Classification of the controlled operators

To generalize the behavior of a U_f-type operator must be enabled to occur phase shifts in addition to the basis changes. Definition 1 defines the behavior of such a generalization for $f \in \mathcal{B}^1$.

Definition 1. $U_{\mathcal{B}^1|n}$ *is the set of n qubit operators such that for each* $V \in U_{\mathcal{B}^1|n}$ *there exist some f, g* $\in \mathcal{B}^1$ *and c, t* $\in \{0, 1, \dots, n-1\}$ *with* $c \neq t$ *where,*

$$V|x\rangle = (-1)^{g(x_t)}|y\rangle$$
$$y_i = \begin{cases} x_i & i \neq t\\ x_i \oplus f(x_c) & i = t\end{cases} \qquad (2)$$

for $x, y \in \mathbb{B}^n$ *and for each* $i \in \{0, 1, \dots, n-1\}$.

More concretely, for $U_{\mathcal{B}^1|n}$ is thought in terms of the four sets of operators, defined relative to the functions in $\mathcal{B}^1$. $U_{\mathrm{B}^1|n} = U_{ZERO|n} \cup U_{ONE|n} \cup\ U_{ID|n} \cup U_{NOT|n}$

Each subset of $U_{\mathcal{B}^1|n}$ contains the operators which correspond to equation 2 relative to the function $f \in \mathcal{B}^1$. This leads to a characterization of $U_{\mathcal{B}^1|n}$ in terms of the two qubit controlled operators.

Theorem 1 *For* $n > 1$,

$$U_{\mathrm{B}^1|n} = \ \{CU_{[c][t]}(A,B)|A,B \in Ext_1 \cup\ Next_1\ and\ \mathrm{c,t} \in \{0{,}1\ \dots, \mathrm{n}-1\}\ \mathrm{c\ c} \neq \mathrm{t}\}$$

Proof. Each of the following theorems can be easily verified using equation1.

1. If A, $B \in \mathrm{Ext}_1$, then $CU_{[c][t]}(A,B) \in U_{ZERO|n}$
2. If A, $B \in N\mathrm{ext}_1$, then $CU_{[c][t]}(A,B) \in U_{ONE|n}$

3. If $A \in \text{Ext}_1$ *and* $B \in Next_1$, then $CU_{[c][t]}(A,B) \in U_{ID|n}$
4. If $A \in Next_1$ *and* $B \in \text{Ext}_1$, then $CU_{[c][t]}(A,B) \in U_{NOT|n}$

Having checked all possible phases of A and B, can be achieved all possible functions for phase encoding in $\mathcal{B}^1$ to satisfy equation 2. If this is done for all pairs of $c, t \in \{0,1,\dots,n-1\}$ and $c \neq t$, it is shown that

$$\{CU_{[c][t]}(A,B) | A,B \in \text{Ext}_1 \cup Next_1, c,t \in \{0,1,\dots,n-1\}, c \neq t\} \subseteq U_{\mathcal{B}^1|n}$$

Furthermore, by covering all possible phases and control/target combinations for each of the four subsets of $U_{\mathcal{B}^1|n}$, it is found that

$$U_{\mathcal{B}^1|n} \subseteq \{CU_{[c][t]}(A,B) | A,B \in \text{Ext}_1 \cup Next_1, c,t \in \{0,1,\dots,n-1\}, c \neq t\}$$

It is easily verified that when $V = CU_{[c][t]}(A,B) \in U_{\mathcal{B}^1|n}$, the effect of V is fully characterized by the parameters c and t, the parameters of A and B, as well as $f \in \mathcal{B}^1$, that corresponds to the subset of $U_{\mathcal{B}^1|n}$, to which V belongs.

$$\langle y|V|x\rangle = \begin{cases} 0 & x \oplus y \notin \{0, 2^t\} \\ (-1)^{\mathcal{E}(A)_{f(x_c)}(x_t)} & x_c = 0 \;\; x \oplus y = f(x_c) * 2^t \\ (-1)^{\mathcal{E}(B)_{f(x_c)}(x_t)} & x_c = 1 \;\; x \oplus y = f(x_c) * 2^t \end{cases} \quad (3)$$

The characterization of $U_{\mathcal{B}^1|n}$ leads to a general specification of the form of their matrix representations.

Theorem 2 *If* $V = CU_{[c][t]}(U(\alpha_A, p_A), U(\alpha_B, p_B))$. *Then:*

For $V \in U_{ZERO|n}$

$$V_{i,j} = \begin{cases} (-1)^{\mathcal{E}(p_A)_0} & i = j \;\; and \;\; i_c = 0 \\ (-1)^{\mathcal{E}(p_B)_0} & i = j \;\; and \;\; i_c = 1 \\ 0 & otherwise \end{cases}$$

For $V \in U_{ONE|n}$ *with target qubit t*

$$V_{i,j} = \begin{cases} (-1)^{\mathcal{E}(p_A)_1} & i \oplus j = 2^t \;\; and \;\; i_c = 0 \\ (-1)^{\mathcal{E}(p_B)_1} & i \oplus j = 2^t \;\; and \;\; i_c = 1 \\ 0 & otherwise \end{cases}$$

For $V \in U_{ID|n}$ *with target qubit t*

$$V_{i,j} = \begin{cases} (-1)^{\mathcal{E}(p_A)_0} & i = j \;\; and \;\; i_c = 0 \\ (-1)^{\mathcal{E}(p_B)_1} & i \oplus j = 2^t \;\; and \;\; i_c = 1 \\ 0 & otherwise \end{cases}$$

For $V \in U_{NOT|n}$ *with target qubit t*

$$V_{i,j} = \begin{cases} (-1)^{\mathcal{E}(p_A)_1} & i \oplus j = 2^t \;\; and \;\; i_c = 0 \\ (-1)^{\mathcal{E}(p_B)_0} & i = j \;\; and \;\; i_c = 1 \\ 0 & otherwise \end{cases}$$

Proof. The proof follows from Theorem 1 and equation 3.

When developing the system for single qubit operators, it was helpful to view them as combinations of their Ext_1 and $Next_1$ basis operators such that the entire action can be accepted as an α degree $Next_1$ and 1 – α degree Et_1operator. In the case of the $U_{\mathcal{B}^1|n}$ operators, a similar thing can be done in terms of the functions of $\mathcal{B}^1$.

For $f \in \mathcal{B}^1$, operator V, which carries out α degree $U_{f|n}$, has the effect described in equation 4. The effect of the operator is partly conditional on f and partly conditional on $\bar{f}$. If e_0, e_1 are functions in $\mathcal{B}^1$, then

$$\langle y|V|x\rangle = \begin{cases} (-1)^{e_0(x_t)}\sqrt{a} & x \oplus y = f(x_c) * 2^t \\ (-1)^{e_1(x_t)}\sqrt{1-a} & x \oplus y = \bar{f}(x_c) * 2^t \\ 0 & otherwise \end{cases} \quad (4)$$

$U_{f|n}$ An α degree effectively acts as a linear combination of two of the elements of $U_{\mathcal{B}^1|n}$: $U_{f|n}$ and $U_{\bar{f}|n}$. There are exactly two forms of the two qubit controlled operators that show this very well defined structure. An α degree $U_{ZERO|n}$ operator is the combination of a $U_{ZERO|n}$ operator with $U_{ONE|n}$, while an $\alpha U_{ID|n}$ operator combines $U_{ID|n}$ with $U_{NOT|n}$.

Degree $\boldsymbol{\alpha}$ operators $\boldsymbol{U_{ZERO|n}}$

A degree α operator $U_{ZERO|n}$ can also be called α a degree (1 - $U_{ONE|n}$) operator. Each operator V *of* this form has the following effect, when applied to basis states.

$$\langle y|V|x\rangle = \begin{cases} (-1)^{e_0(x_t)}\sqrt{a} & x = y \\ (-1)^{e_1(x_t)}\sqrt{1-a} & x \oplus y = 2^t \\ 0 & otherwise \end{cases} \quad (5)$$

First it should be noted that these operators generalize the set of the indexed, formalized operators.

Theorem 3 *If* $\alpha \in$ [0, 1] such that the indexed, formalized operator $A = U_{[t]}(\alpha, \gamma\iota\eta)$. *Then A is an α degree $U_{ZERO|n}$ operator.*
Proof. The proof follows from equation 5 and 3.3.3.1

An indexed operator is a special form of these operators with unconditionally applied phase functions. The condition for carrying out an $\alpha U_{ZERO|n}$, which conditionally applies phase functions is given in theorem 4.

Theorem 4 *For* $\alpha \in$ [0, 1], *let* $A = U(\alpha, (\gamma\iota\eta)_A)$ *and* $B = U(\alpha, (\gamma\iota\eta)_B)$ *be single qubit operators. Then* $C = CU_{[c][t]}(A,B)$ *is an α degree $U_{ZERO|n}$.*

When the phase parameters of both operators are the same then A = B and the two qubit operator C is equivalent to a single qubit, indexed operator. When the phase parameters of A and B differ, then the resultant operation is characterized by conditional encoding and decoding. The perspective for the coding is simple. The sub-operators A and B will encode the information about the target qubit to their respective subspaces, where $x_c = 0$ and $x_c = 1$.

What is perhaps more impressing for the characterization of these operators is their behavior at decoding. If $C = CU_{[c][t]}(A,B)$ is a two qubit operator with operators A and B of the subspace such, that C is an α degree $U_{ZERO|n}$ operator. In such a case the exact action of C is

$$\langle y|V|x\rangle = \begin{cases} (-1)^{\mathcal{E}(A)_0(x_t)}\sqrt{a} & x_c = 0 \;\; and \;\; x = y \\ (-1)^{\mathcal{E}(A)_1(x_t)}\sqrt{1-a} & x_c = 0 \;\; and \;\; x \oplus y = 2^t \\ (-1)^{\mathcal{E}(B)_0(x_t)}\sqrt{a} & x_c = 1 \;\; and \;\; x = y \\ (-1)^{\mathcal{E}(B)_1(x_t)}\sqrt{1-a} & x_c = 1 \;\; and \;\; x \oplus y = 2^t \end{cases} \quad (6)$$

It should be recalled that the requirement for the amplitude at identity decoding is that the amplitude of the decoder to be equivalent to that of the encoder. At the negation decoding the amplitude α_d of the decoder is (1 - α_e), where α_e is the encoding amplitude. Thus for properly chosen α, these operators can carry out conditional identity or negation decoding. The limiting factor here is *that the same type of decoding occurs in both subspaces.* In other words, if an operator carries out an identity decoding in the subspace where the control bit is 0, then it either carries out an identity decoding in the subspace where the control bit is 1 or it does not decode in that subspace.

Degree $\boldsymbol{\alpha}$ operators $\boldsymbol{U_{ID|n}}$

A degree α operator $U_{ID|n}$, similarly to a degree (1 - α) $U_{NT|n}$operator, is characterized by the following formula. If V is a degree α operator $U_{ID|n}$,

$$\langle y|V|x\rangle = \begin{cases} (-1)^{e_0(x_t)}\sqrt{a} & x\oplus y = ID(x_c) * 2^t \\ (-1)^{e_1(x_t)}\sqrt{1-a} & x\oplus y = NOT(x_c) * 2^t \\ 0 & otherwise \end{cases} \qquad (7)$$

The thing that immediately makes an impression is that no subset of these operators can be captured by an unconditional, indexed operator. The indexed operators unconditionally create superpositions where the identity of the input basis has a probability amplitude $\pm\sqrt{\alpha}$. These operators will conditionally set the probability amplitude of basis $|x\rangle$ to be $\sqrt{\alpha}$ or $\sqrt{1-\alpha}$, based on the value of the control bit x_c.

While an α degree $U_{ZERO|n}$ operator requires equivalent amplitude parameters for both subspace operators, an α degree $U_{ID|n}$ operator requires the amplitude to be complementary.

Theorem 5 *For $\alpha \in$ [0, 1], let $A = U(\alpha, (\gamma\iota\eta)_A)$ and $B = U(1-\alpha, (\gamma\iota\eta)_B)$ be single*
qubit operators. Then $C = CU_{[c][t]}(A, B)$ is an α degree $U_{ID|n}$.
Proof. First, let's examine the effect of the subspace operators A and B.
$A_{[t]}|x\rangle = (-1)^{\varepsilon((\gamma\iota\eta)_A)_0}\sqrt{a}|x\rangle + (-1)^{\varepsilon((\gamma\iota\eta)_A)_1}\sqrt{1-a}|x\oplus 2^t\rangle$
$B_{[t]}|x\rangle = (-1)^{\varepsilon((\gamma\iota\eta)_A)_0}\sqrt{1-a}|x\rangle + (-1)^{\varepsilon((\gamma\iota\eta)_A)_1}\sqrt{a}|x\oplus 2^t\rangle$

When $x_c = 0$ (respectively $x_c = 1$), then $A|x\rangle$ (respectively $B|x\rangle$) carries out the desired action for an α degree $U_{ID|n}$ operator. If $C = CU_{[c][t]}(A, B)$ is a two qubit operator with subspace operators $A = U(\alpha_A, p_A)$ *and* $B = U(1-\alpha_B, p_B)$, such that C is an α_A degree $U_{ID|n}$ operator. From there the exact action of C is

$$\langle y|V|x\rangle = \begin{cases} (-1)^{\mathcal{E}(p_A)_0(x_t)}\sqrt{a} & x_c = 0 \ \ and \ \ x = y \\ (-1)^{\mathcal{E}(p_A)_1(x_t)}\sqrt{1-a} & x_c = 0 \ \ and \ \ x\oplus y = 2^t \\ (-1)^{\mathcal{E}(p_B)_0(x_t)}\sqrt{a} & x_c = 1 \ \ and \ \ x = y \\ (-1)^{\mathcal{E}(p_B)_1(x_t)}\sqrt{1-a} & x_c = 1 \ \ and \ \ x\oplus y = 2^t \\ 0 & otherwise \end{cases} \qquad (8)$$

The encoding/decoding action of C is in opposition to that of $U_{ZERO|n}$ degree αoperators. When a $U_{ID|n}$ degree α operator carries out an identity decoding in one subspace, the other subspace is either subject to a negation decoding or is not decoded depending on the seleciton of phase parameters. If operator A is a decoder, then the required amplitude for operator B puts B as an additional decoder with the right choice of phase parameters.

Partially controlled operators

The $U_{\mathcal{B}^1|n}$ degree α operators capture an ordered subset of the controlled operators that can be expressed with equation 1. This well structured subset is computed on very specific relationships between the amplitude parameters for the subspace operators. Thus, the characterization of non-basis controlled operators as the degree α operators does not serve to classify all the possible controlled operators, which might be specified within the formalized system for designing of algorithmic models for quantum circuits. However, it does capture the form of controlled operators encountered in circuits, which are constructed of elementary operators.

If $C = CU_{[c][t]}(A, B)$ for $A, B \in \mathrm{Ext}_1 \cup Next_1$. Then, for an indexed operator *D*, targeting qubit *t*,
$DC = CU_{[c][t]}(AD, BD)$ (9)

From Theorem 5 it clearly follows that DC must be some form of degree $U_{\mathcal{B}^1|n}$ α operator. Given that the CNOT operator, $CU_{[c][t]}(I, X)$ is the only controlled operator needed for the construction of *n* qubit circuits, it follows that equation 9, and therefore the degree $U_{\mathcal{B}^1|n}$ α construction, captures the subset of controlled operators, which might be encountered in the current practice

3 Conclusion

This report examines controlled formalized operators. The two qubit controlled operator defined in equation 1, is more or less the same generalization, which is presented in the previous reports of the author [7, 8, 9]. The research builds on the standard U_f external data sources, for development of a generalized system for conditional operators. This is completed in Theorem 1. Then it was shown in equation 4, how certain controlled operators may be considered as linear combinations of $U_{\mathcal{B}^1|n}$ operators. This system allows for operation with controlled operators and Oracle operators in the same unified system, and in a way, similar to the one, which was used for the single qubit operators. It provides a generalized scheme for the type of the controlled operators, which could be encountered in a circuit, composed entirely of elementary operators.

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.