Generalised quantum weakest preconditions

Roman Gielerak and Marek Sawerwain

Institute of Control and Computation Engineering,
Faculty of Electrical Engineering, Computer Science and Telecommunications,
University of Zielona Góra,
Podgórna 50, 65-246 Zielona Góra, Poland.

Received 18 April 2009

Generalisation of the quantum weakest precondition result of D’Hondt and Panangaden is presented. In particular the most general notion of quantum predicate as positive operator valued measure (POVM) is introduced. The previously known quantum weakest precondition result has been extended to cover the case of POVM playing the role of a quantum predicate. Additionally, our result is valid in infinite dimension case and also holds for a quantum programs defined as a positive but not necessary completely positive transformations of a quantum states.

Contents

1. Introduction 1
2. Formulation of the result 3
3. Summary and conclusions 6
References 6

1. Introduction

The formalism of 0–1 quantum predicates calculus was invented by von Neumann already in 1936 [Birkhoff and Neumann 1936] and [Mackey 1963]. The main discovery was that the corresponding calculus slightly differs from the classical one (which is described in terms of Bool algebra notion) and the discovery of the so-called quantum logic was achieved. In the past there were many activities in this fascinating area (for example see [Piron 1976] and [Dalla Chiara 1977], [Dalla Chiara 2001]).

The recent developments in the quantum information area [Nielsen and Chuang 2000] renewed our interest in creating a general quantum predicate calculus in the context of the recent advances of quantum languages and quantum programming concepts [Sanders and Zuliani 2000], [Betelli et al. 2003] and [Selinger 2004]. In the works [Ömer 2003] and [Ömer 2005] Bernard Ömer introduced the first quantum programming language QCL. Paolo Zuliani also provides tools to compile quantum programs in [Zuliani 2005].

The weakest-precondition (in literature known as the weakest liberal precondition – termed WP) is well-known paradigm of a goal-directed programming methodology
and semantics for a programming language. The weakest-precondition was developed by (de Bakker and de Roever 1972) and (de Bakker and Meertens 1975) and popularised by (Dijkstra 1976). This notion is connected with the Hoare triple \( \{ f_1 \} P \{ f_2 \} \) (Hoare 1969), where \( f_1 \) and \( f_2 \) denote some predicates and \( P \) is the program. In other words, the Hoare triple says: if \( f_1 \) is true for some entry state and after executing \( P \) we obtain the final state, then \( f_2 \) is also true in the final state.

For any program \( p \) and predicate \( f_2 \), we define the predicate \( WP(p, f_2) \) as

\[
s \models WP(p, f_2) = \forall t \in S_p \ p(s) \rightarrow t \Rightarrow (t \models f_2)
\]  

The WP is the weakest precondition operator and the predicate \( WP(p, f_2) \) is the weakest one satisfying the Hoare triple \( \{ WP(p, f_2) \} P \{ f_2 \} \). The Hoare triple can be expressed with the wp operator \( s \models f_1 \Rightarrow WP(p, f_2) \).

The strongest postcondition (termed SP) is defined by

\[
t \models SP(p, f_1) = \exists s \in S_p \ p(s) \rightarrow t \land s \models f_1.
\]  

From the definition of the Hoare triple we obtain that \( \models SP(p, f_1) \Rightarrow f_2 \) is equivalent to \( \{ f_1 \} p \{ f_2 \} \).

In the work (D’Hondt and Panangaden 2006) the existence of weakest precondition for quantum predicates defined as hermitian operators with trace smaller than one was presented. However, the Krauss representation for completely positive finite dimensional superoperators was used in their proof in a very essential way, what is more the proof in (D’Hondt and Panangaden 2006) is valid in the situation when the following conditions are satisfied:

**HP(1)** the considered quantum systems are finite-dimensional,

**HP(2)** the allowed quantum programs are defined as a completely positive transformations,

**HP(3)** the admissible predicates are defined as finite dimensional hermitian operators with trace smaller than one.

However, in many realistic situations all the listed assumptions HP(1)–HP(3) made in (D’Hondt and Panangaden 2006) are too restrictive. For example, the serious candidate for the realistic quantum computer, the computing machine with coherent pulses of light (Ralph et al. 2003) is the point where infinite dimensional character of the corresponding quantum registers comes into play. Secondly, the major role played by the very notion of predicates is to control the evolution of the state of quantum register. There the well known problems connected with quantum measurements do occur. In particular the possible noisy character of quantum measurement is definitely excluded from the consideration by HP(3). In other words, the condition HP(3) restricts our considerations essentially to the orthodox von Neumann type of measurement only. Finally, although there are very plausible arguments in favour of completely positive maps as the only realistic transformation of the corresponding spaces of quantum states (the possible occurrence of positive maps in non-unitary quantum evolution is not definitely excluded (Majewski 2007)).

In this paper we demonstrate result on the existence of the quantum weakest preconditions to cover the situations where none of the assumptions HP(1)–HP(3) are fulfilled.
The main result is formulated precisely as Theorem 2.1 in Sec. 2. What is surprising, the proof of our slight generalisation of theorem due to (D'Hondt and Panangaden 2006) is very simple. The main argument is the use of Hilbert-Schmidt duality instead of Krauss representation as it was done in (D'Hondt and Panangaden 2006).

2. Formulation of the result

Let \( \Sigma \subset \mathbb{R}^d \) be a Borel measurable subset of \( d \)-dimensional Euclidean space \( \mathbb{R}^d \) and let \( \mathcal{H} \) be a separable complex Hilbert space. \( \mathcal{L}(\mathcal{H}) \) will stand for linear continuous operators on \( \mathcal{H} \). The \( \sigma \)-algebra of sets of \( \Sigma \) is denoted as \( \beta(\Sigma) \).

A positive operator valued measure (POVM) on \((\Sigma, \beta(\Sigma))\) is a \( \sigma \)-additive map \( F : \beta(\Sigma) \rightarrow \mathcal{L}(\mathcal{H}) \) and \( ||F\Sigma|| \leq 1 \). The space of such measurements will be denoted as \( \text{POVM}(\Sigma, \mathcal{H}) \).

A natural partial order \( \preceq \) can be defined in \( \text{POVM}(\Sigma, \mathcal{H}) \). Let \( F, G \in \text{POVM}(\Sigma, \mathcal{H}) \) then \( F \preceq G \) iff \( \forall A \in \beta(\Sigma) \) \( F(A) = F_A \preceq G_A = G(A) \) (4) where \( \preceq \) is the natural ordering relation in \( \mathcal{L}(\mathcal{H}) \) i.e. \( F_A \preceq G_A \iff \forall \psi \in \mathcal{H} \langle \psi | F_A \psi \rangle \leq \langle \psi | G_A \psi \rangle \) (5)

Lemma 2.1. For any Borel \( \Sigma \subset \mathbb{R}^d \) the partially ordered space denoted as \( \text{(POVM}(\Sigma, \mathcal{H}), \preceq \) ) is completely partially ordered space (cpos).

Proof. Let \((F^{(\alpha)})_{\alpha \in A}\) be any \( \alpha \)-ordered net in \( \text{POVM}(\Sigma, \mathcal{H}) \). For any \( |\psi\rangle \in \mathcal{H} \), \( A \in \Sigma \) we define

\[ \langle \psi | G_A \psi \rangle = \sup_{\alpha} \langle \psi | F_A^{(\alpha)} \psi \rangle. \] (6)

From the assumption on the uniform boundness of elements from \( \text{POVM}(\Sigma, \mathcal{H}) \) and the polarisation identities it follows that \( F \) defines an operator \( G_A \) and such that \( ||G_A|| \leq 1 \).

Let \((A_n)_{n=1,\ldots,\infty}\) be any family of pairwise disjoint subsets of \( \beta(\Sigma) \), then the use of the version of the dominated convergence theorem allows us to formulate

\[ G_{\bigcup_{n=1}^{\infty} A_n} = \Sigma_{n=1}^{\infty} G_{A_n} \] (7)

in the strong sense and thus because of uniform boundness in operator norm topology. In conclusion, the operator valued map

\[ A \in \beta(\Sigma) \longrightarrow G_A \in \mathcal{L}(\mathcal{H}) \] (8)

defines POVM as shown above.

By the (generalised) quantum predicate we mean an arbitrary element \( F \in \text{POVM}(\Sigma, \mathcal{H}) \) with the additional property that for any \( A \in \beta(\Sigma) \) the corresponding operator \( F_A \) is trace class and moreover \( \text{Tr}(F_A) \leq 1 \). The (closed) subset of such POVM-s will be denoted as \( \text{Pre}(\Sigma, \mathcal{H}) \).

For a given separable Hilbert space \( \mathcal{H} \) the corresponding space of states \( E(\mathcal{H}) \) is usually defined as the set of non-negative, trace-class operators \( \rho \) and such that \( \text{Tr}(\rho) = 1 \). A space
of admissible transformations of the space $E(\mathcal{H})$ is defined as the space of linear positivity preserving maps:

$$C : E(\mathcal{H}) \rightarrow E(\mathcal{H})$$

that are trace preserving.

Any such map will be called (generalised) quantum program and the space of all such maps will be denoted as $\text{QP}(\mathcal{H})$.

It is well known that the ring of trace-class operators on $\mathcal{H}$ denoted as $L_1(\mathcal{H})$ forms two-sided $*$-ideal in the $C^*$-algebra $L(\mathcal{H})$ and therefore for any $\rho \in E(\mathcal{H})$, $F \in \text{Pre}(\Sigma, \mathcal{H})$ and $C \in \text{QP}(\mathcal{H})$:

$$\text{Tr}_\mathcal{H}(FA_C(\rho)) \leq 1$$

The last equation allow to formulate the following lemma.

**Lemma 2.2.** For any $C \in \text{QP}(\mathcal{H})$ the action $C^*$ on $\text{Pre}(\Sigma, \mathcal{H})$ is defined by:

$$\forall \rho \in E(\mathcal{H}) \rightarrow C^*F \in \text{Pre}(\Sigma, \mathcal{H})$$

where

$$\forall \rho \in E(\mathcal{H}) \text{ Tr}(C^*F_A \rho) = \text{Tr}(FA_C(\rho))$$

is action of $\text{QP}(\mathcal{H})$ on the space $\text{Pre}(\Sigma, \mathcal{H})$.

**Proof.** From $\rho \in L_1(\mathcal{H})$ and the spectral theorem it follows $\rho = \Sigma_n \lambda_n |\psi_n\rangle \langle \psi_n|$, $\lambda_n \geq 0$, $\lim_{n \to \infty} \lambda_n = 0$ and it is enough to assume that $\rho = |\psi\rangle \langle \psi|$ for some $|\psi\rangle \in \mathcal{H}$ with $|\langle \psi | \psi \rangle| = 1$.

Therefore, the polarisation identities shows that the identities:

$$\langle \psi | (C^*F_A) \psi \rangle = \text{Tr}(F_A C(|\psi\rangle \langle \psi|))$$

define a bounded operator $C^*F$ for any $A \in \beta(\Sigma)$. The $\sigma$-additivity of $C^*F$ and trace properties are also easy to prove. □

The duality between $L(\mathcal{H})$ and $L_1(\mathcal{H})$ based on $\text{Tr}$ will be called Hilbert-Schmidt duality and will be also denoted as

$$\langle \cdot | \cdot \rangle_{HS} : (\rho, A) \in L_1(\mathcal{H}) \times L(\mathcal{H}) \rightarrow \langle \rho | A \rangle_{HS} = \text{Tr}(\rho A)$$

**Definition 2.1.** For a given $\mathcal{H}$, $F \in \text{Pre}(\Sigma, \mathcal{H})$, $\rho \in E(\mathcal{H})$ the function

$$\text{sat}(\rho, F) : A \in \Sigma \rightarrow \text{sat}(\rho, F_A) = \text{Tr}(\rho F_A)$$

will be called the satisfiability of the quantum predicate $F$ in the state $\rho$. In particular the state $\rho$ satisfies the predicate $F$ iff the function $\text{sat}(\rho, F)$ is nonzero positive value.

From def. (2.1) it follows that the function of satisfiability $\text{sat}(\rho, F)$ is always a bounded measure on $\beta(\Sigma)$.

**Definition 2.2.** A $s$-order, denoted as $\preceq$ is defined on the space of quantum predicates $\text{Pre}(\Sigma, \mathcal{H})$ in the following way:

$$F \preceq G \text{ iff } \forall A \in \beta(\Sigma) \forall \rho \in E(\mathcal{H}) \text{ sat}(\rho, F)(A) \leq \text{sat}(\rho, G)(A)$$
Similarly, it can be proved that the semi-ordered space \((\text{Pre}(\Sigma, \mathcal{H}), \preceq)\) is cpos.

**Lemma 2.3.** For \(\Sigma \subseteq \mathbb{R}^d\) and separable Hilbert space \(\mathcal{H}\) the semi-ordered space denoted as \((\text{Pre}(\Sigma, \mathcal{H}), \preceq)\) is completely partially ordered space.

For a given quantum predicate \(F \in \text{Pre}(\Sigma, \mathcal{H})\) the set of preconditions for \(F\) with respect to quantum program \(C \in \text{QP}(\mathcal{H})\) and denoted as \(\{C\}(F)\) is defined as:

\[
\{C\}(F) = \{G \in \text{Pre}(\Sigma, \mathcal{H}) : G \preceq F\}
\]  

(17)

**Definition 2.3.** A weakest precondition for a predicate \(F \in \text{Pre}(\Sigma, \mathcal{H})\) with respect to a quantum program \(C \in \text{QP}(\mathcal{H})\) and denoted (if exists) as \(\text{WP}(C)(F)\) is the predicate \(G \in \text{Pre}(\Sigma, \mathcal{H})\) such that \(G = \text{WP}(C)(F) = \text{sup}(\{C\}(F))\).

**Theorem 2.1.** Let \(\mathcal{H}\) be a separable Hilbert space and let \(C \in \text{QP}(\mathcal{H})\) be a given quantum program and let \(F \in \text{Pre}(\Sigma, \mathcal{H})\). Then there exists an unique \(G \in \text{Pre}(\Sigma, \mathcal{H})\) such that

\[
G = \text{WP}(C)F
\]  

(18)

**Proof.** By taking \(A \in \beta(\Sigma)\), we can write

\[
\text{Tr}(F(A)C(\rho)) = \langle F_A | C\rho \rangle_{\mathcal{H}\mathcal{S}(\mathcal{H})} = \langle C^* F_A | \rho \rangle_{\mathcal{H}\mathcal{S}(\mathcal{H})}.
\]  

(19)

By the Hilbert-Schmidt duality we can define a new POVM\((C^*F)\) on \((\Sigma, \mathcal{H})\) by the last identity. Thus, we can expect that \(C^*F = \text{WP}(C)F\).

Let \(H \in \{C\}(F)\), then for some \(A \in \beta(\Sigma)\)

\[
\text{Tr}(H_A \rho) \leq \text{Tr}(F_A C(\rho)) = \langle F_A | C\rho \rangle_{\mathcal{H}\mathcal{S}(\mathcal{H})} = \langle C^* F_A | \rho \rangle_{\mathcal{H}\mathcal{S}(\mathcal{H})} = \text{Tr}(C^* F_A) \rho
\]  

(20)

and

\[
\text{sat}(H, \rho) \leq \text{sat}(C^* F, \rho)
\]  

(21)

then \(C^*F\) is majorising for the set \(\{C\}F\). Obviously, from the very construction of \(C^*F\) it follows that \(C^*F \in \{C\}F\).

**Remark 2.1.** The action of CP(\(H\)) on the spaces POVM(\(H\)) were studied more carefully in \(\text{(Buscemi et al. 2005)}\) and some very interesting results on this were obtained. Whether those results can be extended to the action of QP(\(H\)) and whether this sort of results could be efficient in the quantum programming area and in our opinion it deserves for further studies.

**Remark 2.2.** The theorem presented in work \(\text{(D’Hondt and Panangaden 2006)}\) is a special case of our theorem \(2.1\). If we assume that the quantum predicate is given by the corresponding \(F \in \text{POVM}(\Sigma, \mathcal{H})\) with one atom support,

\[
F = \{F_1\}
\]  

(22)

then our theorem gives (still with some generalisation) the D’Hondt and Panangaden result.
3. Summary and conclusions

The most general notion of quantum predicate using the notion (connected to a priori noisy measurement process) of positive operator valued measures has been introduced in this note.

The existence of the corresponding quantum weakest preconditions has been proved. Additionally, our result is valid in infinite dimensional situations and for positive but not necessary completely positive quantum programs.

It would be of great importance to provide some examples showing that our generalised quantum predicate notion can be used for semantic analysis of quantum programs. Especially important seems is to be the question of providing interesting examples where previously known tools and results are not directly applicable. It will be a main topic of a forthcoming paper [Gielerak and Sawerwain].

References

de Bakker J. W., de Roever W. P. (1972): A calculus for recursive programs schemes. — In: Automata, Languages, and Programming, Amsterdam, North-Holland, pp. 167–196.
de Bakker J. W., Meertens, L. G. L. T. (1975): On the completeness of the inductive assertion method. — J. Comput. Syst. Sci. Vol. 11, No. 3, pp. 323-357.
Betelli S., Serafini L. and Calarco T. (2003): Toward an architecture for quantum programming.
— Eur. Phys. J., 25:181–200, arXiv:cs/0103009
Birkhoff G., von Neumann J. (1936): The Logic of Quantum Mechanics. — Ann. Math., Vol. 37, pp. 823-843.
Buscemi F., DAriano G.M., Keyl M., Perinotti P., Werner R.F. (2005): Clean positive operator valued measures. — Journal of Mathematical Physics, Vol. 46, Issue 8, p.082109, arXiv:quant-ph/0505095
Dalla Chiara, M.L. (2001): Quantum logic. — in: D.M. Gabbay, F. Guenthner (Eds.), Handbook of Philosophical Logic, Vol. III, 1986, pp. 427–469. Revised version in: Handbook of Philosophical Logic, Vol. 6, 2nd edn., Kluwer, Dordrecht, pp. 129–228.
Dalla Chiara M.L. (1977): Quantum logic and physical modalities. — J. Philos. Logic 6, pp. 391–404.
Choi M.D. (1975): Completely positive linear maps on complex matrices. — Linear Algebra and its Applications, Vol. 10, pp. 285–290.
Dijkstra E. W. (1976): A Discipline of Programming. — Prentice-Hall, Englewood Cliffs, N.J. .
Gielerak R., Sawerwain M.: General quantum predicate as semantics tools in quantum programming theory. — in preparation.
Hoare C. (1969): An axiomatic basis for computer programming. — Communications of the ACM, Vol. 12, pp. 576–583.
D’Hondt, E., Panangaden, P. (2006): Quantum weakest preconditions. — Mathematical Structures in Computer Science, Vol. 16, No. 3, pp. 429–451.
Kraus K. (1983): State, Effects, and Operations. — Berlin, Springer-Verlag.
Mackey G. (1963): Mathematical foundations of Quantum Mechanics. — W.A. Benjamin.
Majewski W.A. (2007): On non-completely positive quantum dynamical maps on spin chains. — Phys. A: Math. Theor. 40, pp. 11539-11545, arXiv:quant-ph/0606176
Nielsen M., Chuang I. L. (2000): Quantum Computation and Quantum Information. — Cambridge University Press.
Ömer B. (2003): *Structured Quantum Programming*. — PhD thesis, Technical University of Vienna, Austria.

Ömer B. (2005): *Classical Concepts in Quantum Programming*. — Int. J. of The. Phys., Vol. 44, No. 7, pp. 943–955.

Piron P. (1976): *Foundations of Quantum Physics*. — W. A. Benjamin.

Ralph T. C., Gilchrist A., Milburn G. J., Munro W. J., Glancy S. (2003): *Quantum computation with optical coherent states*. — Phys. Rev. A, Vol. 68, 042319.

Sanders J. W., Zuliani P. (2000): *Quantum programming*. — In Mathematics of Program Construction, Springer LNCS 1837, pp. 80–99.

Selinger P. (2004): *Towards a quantum programming language*. — Mathematical Structures in Computer Science, 14(4):527-586.

Zuliani P. (2005): *Compiling quantum programs*. — Acta Informatica, 41(7-8):435–474.