

On the solution of linear matrix equations

Technical note 0401, version 1

Michael A. Nielsen^{1,*}

¹*School of Physical Sciences and School of Information Technology and Electrical Engineering,
The University of Queensland, Brisbane, Queensland 4072, Australia*

(Dated: June 6, 2004)

We study the solution of linear matrix equations $\mathcal{L}(X) = C$, introducing a powerful tool, the vec operation, which greatly simplifies the solution of such equations. We illustrate the use of vec with applications to problems such as finding the fixed point of a quantum operation, and quantum process tomography. We conclude with *Shoda's first and second theorems*, which characterize when a matrix M can be written as an additive commutator, $M = [X, Y]$, and as a multiplicative commutator, $M = XYX^{-1}Y^{-1}$, respectively.

I. OVERVIEW

These notes study the problem of finding solutions to linear matrix equations like $AX + XB = C$. At first sight this may appear to be somewhat dry problem, but we'll see that it has many important applications in physics. Examples include *quantum process tomography* [1, 2] and the Solovay-Kitaev theorem [3, 4]. The notes are based largely on material from Chapter 4 of Horn and Johnson's "Topics in Matrix Analysis" [5]; further historical information on the results presented may be obtained in that source.

II. THE OPERATION vec

The key tool in our study is a simple, apparently innocuous mathematical operation named vec . The vec operation is applied to a matrix, and produces as output the vector formed by stacking all the columns of the matrix up on top of one another. More formally, let $M_{m,n}$ denote the space of $m \times n$ complex matrices. Let $A \in M_{m,n}$. Then we define $\text{vec}(A)$ to be the mn -dimensional vector formed by stacking all the columns of A up on top of one another. For example, we have:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow \text{vec}(A) = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}. \quad (1)$$

We call $\text{vec}(A)$ the *vectorized* form of the matrix A .

Why define vec ? The answer is that it provides an algebraically and computationally convenient way of making explicit the structure of $M_{m,n}$ as a *vector space*. The rest of this note can be viewed as an attempt to make this point in a more precise fashion, but let's try to get the flavour by looking at a simple example.

Observe that solving the linear equation $AX + XB = C$ is equivalent to simultaneously satisfying all the linear

equations $\sum_k (A_{jk}X_{kl} + X_{jk}B_{kl}) = C_{jl}$. We could solve these equations directly on a computer. However, introducing the $\text{vec}(X)$ notation for the vector whose entries are the X_{jk} turns out to simplify the problem greatly. We'll see that $AX + XB = C$ is equivalent to the much more transparent equation $(I \otimes A + B^T \otimes I)\text{vec}(X) = \text{vec}(C)$, whose solution can be obtained and understood using the usual techniques of matrix analysis. The reason for this equivalence is some beautiful algebraic properties of vec that greatly simplify the analysis of equations like $AX + XB = C$. As is so often the case in mathematics, there is a considerable advantage in formalizing an operation, and then studying the algebraic properties of that formalization.

The key algebraic fact about vec can be understood physically as a connection with maximally entangled states. Let $A \in M_{m,n}$, and let quantum systems Q_1 and Q_2 both have dimension n . Define the (unnormalized) maximally entangled state of Q_1Q_2 by

$$|ME_n\rangle \equiv \sum_j |j\rangle|j\rangle \quad (2)$$

where the $|j\rangle$ are fixed orthonormal bases for systems Q_1 and Q_2 , respectively. (We won't bother to distinguish the two bases notationally, although they are, of course, distinct bases.) Regarding the matrix A as being defined in the basis $|j\rangle$ for Q_2 , we have the remarkable identity

$$\text{vec}(A) = (I_n \otimes A)|ME_n\rangle, \quad (3)$$

where I_n is the $n \times n$ identity matrix. We will omit the subscript n when its value is clear from context. To prove Eq. (3) note that by linearity it suffices to prove the identity when $A = |j\rangle\langle k|$. The proof is completed by verifying that $\text{vec}(|j\rangle\langle k|) = |k\rangle|j\rangle$ and $(I \otimes |j\rangle\langle k|)|ME_n\rangle = |k\rangle|j\rangle$.

The operation vec has many useful properties, some of which we collect here. All are easily proved, so we omit the proofs.

1. If $A, B \in M_{m,n}$ then $\text{vec}(A) = \text{vec}(B)$ if and only if $A = B$.
2. For every mn -dimensional vector v there exists a unique matrix $M \in M_{m,n}$ such that $\text{vec}(M) = v$.

*nielsen@physics.uq.edu.au and www.qinfo.org/people/nielsen

3. The inner product $\text{vec}(A)^\dagger \cdot \text{vec}(B) = \text{tr}(A^\dagger B)$.
4. The Schmidt number of $\text{vec}(A)$ is equal to the rank of A .
5. $\text{vec}(A \otimes B) = \text{vec}(A) \otimes \text{vec}(B)$, with respect to an appropriate ordering of the factors in the tensor product.

III. ROTH'S LEMMA

The identity Eq. (3) has an extremely useful generalization, which Horn and Johnson ascribe to Roth [6].

Lemma 1 (Roth's lemma). *When $A \in M_{l,m}, B \in M_{m,n}, C \in M_{n,p}$, we have*

$$\text{vec}(ABC) = (C^T \otimes A)\text{vec}(B). \quad (4)$$

Proof: We have $\text{vec}(ABC) = (I_p \otimes ABC)|ME_p\rangle$. A calculation shows that $(I_p \otimes C)|ME_p\rangle = (C^T \otimes I_n)|ME_n\rangle$, and so

$$\text{vec}(ABC) = (C^T \otimes AB)|ME_n\rangle \quad (5)$$

$$= (C^T \otimes A)(I_n \otimes B)|ME_n\rangle \quad (6)$$

$$= (C^T \otimes A)\text{vec}(B). \quad (7)$$

QED

IV. APPLICATION OF vec TO THE SOLUTION OF MATRIX EQUATIONS

Roth's lemma makes it straightforward to solve linear matrix equations. For example, we immediately see that the equation $AX + XB = C$ is equivalent to the vector equation

$$(I \otimes A + B^T \otimes I)\text{vec}(X) = \text{vec}(C). \quad (8)$$

The solution to this vector equation is easily obtained using standard techniques of matrix analysis. These techniques are well-known, so I won't talk about them in much detail, except to give one example for flavour. Suppose we are searching for solutions to the equation $AX + XB = 0$. This is equivalent to $(I \otimes A + B^T \otimes I)\text{vec}(X) = 0$, i.e., to $\text{vec}(X)$ being in the kernel of $I \otimes A + B^T \otimes I$. We can see that a solution to the equation exists if and only if there are eigenvalues λ_a of A and λ_b of B such that $\lambda_a = -\lambda_b$. Indeed, when A and B are normal operators the dimensionality of the kernel is easily calculated using standard techniques; to solve the more general case we need to do some work on tensor products and the Jordan canonical form, but this is still relatively straightforward matrix analysis.

More generally, an arbitrary linear matrix equation may be written in the form $\sum_j A_j X B_j = C$. From

Roth's lemma, we see that this is equivalent to the equation

$$\sum_j (B_j^T \otimes A_j)\text{vec}(X) = \text{vec}(C), \quad (9)$$

which may be solved using standard techniques.

This discussion suggests a useful new abstraction: a vectorized form for a linear operation on matrices. In particular, given a linear operation $\mathcal{L}(\cdot)$ on matrices, we can define a vectorized form of \mathcal{L} as follows. First, note that \mathcal{L} can always be written in the form $\mathcal{L}(X) = \sum_j A_j X B_j$, for some set of matrices A_j and B_j . Then the vectorized form $\text{vec}(\mathcal{L})$ is defined by

$$\text{vec}(\mathcal{L}) \equiv \sum_j B_j^T \otimes A_j. \quad (10)$$

It is not difficult to show that $\text{vec}(\mathcal{L})$ defined in this way is unique, i.e., it does not depend on the particular representation in terms of a set of A_j and B_j operators. Note that we have

$$\text{vec}(\mathcal{L})\text{vec}(X) = \text{vec}(\mathcal{L}(X)). \quad (11)$$

The notation $\text{vec}(\mathcal{L})$ is not, so far as I know, a standard notation. It is arguably the case that we should really write $\text{mat}(\mathcal{L})$, since $\text{vec}(\mathcal{L})$ is, of course, a matrix, not a vector. That is, the operation vec *matrixizes* the linear operation \mathcal{L} . Nonetheless, I will stick with the notation $\text{vec}(\mathcal{L})$ here.

V. VECTORIZING QUANTUM OPERATIONS

As an application of these ideas, consider the trace-preserving quantum operation

$$\mathcal{E}(\rho) = \sum_j E_j \rho E_j^\dagger. \quad (12)$$

From results of Ruskai [7] it can be shown that such an operation always has at least one (and possibly more) fixed points. How can we find these fixed points? An easy way is to vectorize the operation \mathcal{E} , from which we see that a fixed point ρ satisfies

$$\text{vec}(\mathcal{E})\text{vec}(\rho) = \text{vec}(\rho), \quad (13)$$

where $\text{vec}(\mathcal{E}) = \sum_j E_j^* \otimes E_j$. Thus, the fixed points of \mathcal{E} may be obtained by solving for the eigenvalue 1 subspace of $\text{vec}(\mathcal{E})$.

Another entertaining application of vec is to understand the freedom in the operation elements E_j appearing in the operator-sum representation. This freedom is well-known to quantum information theorists; it is reviewed, for example, on page 372 of [4]. The basic idea is to suppose \mathcal{E} can be written as $\mathcal{E}(\rho) = \sum_j E_j \rho E_j^\dagger = \sum_k F_k \rho F_k^\dagger$ for two different sets of operation elements E_j

and F_k . It is a simple and worthwhile exercise in using vec to understand the necessary and sufficient conditions on the relationship of the E_j and the F_k . The details are left to the reader.

Conjecture: It is tempting to conjecture that $\|\text{vec}(\mathcal{E})\| \leq 1$. This is equivalent to the statement that \mathcal{E} is contractive with respect to the Hilbert-Schmidt norm on operators, a result which I have doubts about, but which would nicely complement Ruskai's result [7] that \mathcal{E} is contractive with respect to the trace norm. It is straightforward to verify this conjecture when \mathcal{E} is unitary, when \mathcal{E} is a single-qubit operation, and when \mathcal{E} is a convex combination of operations known to satisfy the conjecture¹. Given this wide range of applicability, either a proof or a counterexample would have some interest.

Problem: Characterize the class of vectors $\text{vec}(\rho)$, where ρ is a density matrix. An easily-proved but not entirely satisfactory characterization is that these are the vectors $|\rho\rangle = \text{vec}(\rho)$ satisfying $\langle ME|\rho\rangle = 1$ and $\langle\psi^*|\langle\psi|\rho\rangle \geq 0$ for all $|\psi\rangle$. Note also that the set $\text{vec}(\rho)$ is a convex set.

Problem: Characterize the class of matrices which can be written in the form $\sum_j E_j^* \otimes E_j$.

Problem: Characterize the class of matrices $\text{vec}(L)$ corresponding to a positivity-preserving linear map \mathcal{L} .

VI. VECTORIZING QUANTUM PROCESS TOMOGRAPHY

The ideas we have described can be fruitfully applied to the problem of quantum process tomography. Suppose $\rho_1, \dots, \rho_{d^2}$ is a set of linearly independent density matrices that forms a complete basis for the space of $d \times d$ matrices. Suppose that we are able to experimentally prepare these states, apply a process \mathcal{E} , and then use state tomography to determine the outputs $\rho'_j \equiv \mathcal{E}(\rho_j)$. Suppose we define

$$\tilde{\rho} \equiv [\text{vec}(\rho_1) \dots \text{vec}(\rho_{d^2})] \quad (14)$$

$$\tilde{\rho}' \equiv [\text{vec}(\rho'_1) \dots \text{vec}(\rho'_{d^2})]. \quad (15)$$

Then we have

$$\text{vec}(\mathcal{E})\tilde{\rho} = \tilde{\rho}'. \quad (16)$$

But $\tilde{\rho}$ is invertible since the set $\rho_1, \dots, \rho_{d^2}$ is linearly independent and spans the entire space of $d \times d$ matrices. It follows that we can extract $\text{vec}(\mathcal{E})$ via

$$\text{vec}(\mathcal{E}) = \tilde{\rho}'\tilde{\rho}^{-1}. \quad (17)$$

The equation Eq. (17) gives us a simple procedure for obtaining $\text{vec}(\mathcal{E})$ from experimental data. Is there a way of obtaining \mathcal{E} in a more conventional form than $\text{vec}(\mathcal{E})$?

Suppose we choose a basis E_j of operators orthonormal with respect to the trace inner product, i.e., $\text{tr}(E_j^\dagger E_k) = \delta_{jk}$. Then we can always expand \mathcal{E} as

$$\mathcal{E}(\rho) = \sum_{jk} \chi_{jk} E_j \rho E_k^\dagger, \quad (18)$$

where χ_{jk} is a set of complex numbers known as the *chi matrix* for the quantum operation \mathcal{E} . The vectorized form of \mathcal{E} is related to the chi matrix via the equation

$$\text{vec}(\mathcal{E}) = \sum_{jk} \chi_{jk} E_k^* \otimes E_j, \quad (19)$$

so χ can be extracted from $\text{vec}(\mathcal{E})$ by computing:

$$\chi_{jk} = \text{tr} \left((E_k^T \otimes E_j^\dagger) \text{vec}(\mathcal{E}) \right). \quad (20)$$

Equations (17) and (20) together give a simple procedure for extracting the chi matrix from experimental data.

VII. SHODA'S THEOREMS

A square matrix $M \in M_{n,n}$ that can be written in the form $M = [X, Y] = XY - YX$ is called an *additive commutator*. A square matrix $M \in M_{n,n}$ that can be written in the form $M = XYX^{-1}Y^{-1}$ is called a *multiplicative commutator*. Shoda's theorems provide a simple way of testing whether a matrix is an additive or a multiplicative commutator.

Theorem 1 (Shoda's first theorem). *A matrix $M \in M_{n,n}$ is an additive commutator if and only if $\text{tr}(M) = 0$.*

Shoda's first theorem tells us when the equation $M = [X, Y]$ has solutions X and Y . The ability to construct such solutions X and Y is important, for example, in the proof of the Solovay-Kitaev theorem. We will see in the proof that if M is Hermitian then it is possible to choose X and Y to be Hermitian also.

Proof: The forward implication follows from the cyclic property of trace. How should we approach the proof of the reverse implication? The obvious approach is to try to guess appropriate solutions X and Y . Parameter counting tells us that if there are any solutions X and Y , then there are likely to be many solutions X and Y . This suggests that we start by making a guess for X in some particularly simple and convenient form, and then attempt to solve for Y .

How should we choose X ? The simplest form is $X \propto I$, but this gives $[X, Y] = 0$. Let's try something a little more complicated, choosing X diagonal with entries x_1, \dots, x_n . We have

$$[X, Y]_{jk} = Y_{jk}(x_j - x_k). \quad (21)$$

If we can choose Y_{jk} so that $M_{jk} = Y_{jk}(x_j - x_k)$ then $[X, Y] = M$. It is easy to see that this is always possible, provided M has zeroes on the diagonal.

¹ This thus includes convex combinations of unitary operations.

To complete the proof we need a lemma, proved below, stating that every traceless M can be written in the form $M = U\tilde{M}U^\dagger$, where U is unitary and \tilde{M} has zeroes on the diagonal. It follows that there exist X and Y such that $\tilde{M} = [X, Y]$ and thus $M = [UXU^\dagger, UYU^\dagger]$.

QED

Lemma 2. *Let $M \in M_{n,n}$ be traceless. Then there exists a unitary U such that UMU^\dagger has zero entries on the diagonal.*

Proof: Let F_k be any $k \times k$ unitary whose first column is uniformly $1/\sqrt{k}$, e.g., the Fourier transform. Define the $n \times n$ unitary $G_k \equiv I_k \oplus F_{n-k}$. A calculation shows that the first diagonal entry of $G_0MG_0^\dagger$ is zero. A similar calculation shows that the first two diagonal entries of $G_1G_0MG_0^\dagger G_1^\dagger$ are zero. Similarly, we see that $G_{n-1} \dots G_0MG_0^\dagger \dots G_{n-1}$ has all zeroes on its diagonal, which completes the proof.

There is an interesting alternate proof of this lemma using majorization when M is Hermitian. Observe that the zero vector is majorized by the vector d of diagonal entries in M . Horn's lemma [8, 9, 10] ensures the existence of a unitary U such that $0 = \sum_k |U_{jk}|^2 d_j$. It follows that UMU^\dagger has zeroes on its diagonal.

QED

Theorem 2 (Shoda's second theorem). *A matrix $M \in M_{n,n}$ is a multiplicative commutator if and only if $\det(M) = 1$.*

This result can be thought of as the Lie group analogue of Shoda's first theorem. Presumably these types of results can be generalized to more general Lie algebras and Lie groups.

Proof: The forward implication follows from the fact that \det is a homomorphism, i.e., $\det(AB) = \det(A)\det(B)$. I don't yet fully understand the proof of the reverse implication, but can prove the result for the special case when M is normal. Suppose first that M is diagonal, $M = \text{diag}(m_1, \dots, m_n)$. We choose a basis $|0\rangle, \dots, |n-1\rangle$ for the vector space, and choose X to act as the displacement operator, $X|j\rangle \equiv |j \oplus 1\rangle$, where \oplus indicates addition modulo n . We select $Y = \text{diag}(y_1, \dots, y_n)$, so

$$XYX^{-1}Y^{-1} = \text{diag}\left(\frac{y_n}{y_1}, \frac{y_1}{y_2}, \dots, \frac{y_{n-1}}{y_n}\right). \quad (22)$$

We now simply choose the y_j so that $y_{j-1}/y_j = m_j$; this can always be done, since $\det(M) = 1$. The result for an arbitrary normal matrix M follows by expressing $M = U\tilde{M}U^\dagger$, where U is unitary and \tilde{M} is diagonal, so that $\tilde{M} = XYX^{-1}Y^{-1}$ and thus $M = X'Y'X'^{-1}Y'^{-1}$, where $X' = UXU^\dagger, Y' = UYU^\dagger$.

QED

There is an entertaining use of this proof in quantum circuit design. Suppose one wishes to obtain a controlled- U operation, where $U \in su(2)$. If U is diagonal then the proof of the result tells us that we can obtain the controlled- U gate by doing the following sequence of operations: (1) Y^{-1} on the target qubit; (2) a controlled-NOT; (3) Y on the target qubit; and (4) a controlled-NOT. This type of construction is crucial in proving the universality of controlled-NOT and single-qubit unitaries. A nice fact about the present proof is that it is easily extended to *qudit* systems, and can be used to show, for example, that the controlled-displacement operation, together with single-qudit unitaries, is universal for quantum computation on qudit systems.

VIII. SUMMARY

Summary of material covered: definition of vec ; formula for vec in terms of maximally entangled states; Roth's lemma; using Roth's lemma to solve linear matrix equations; definition of $\text{vec}(\mathcal{L})$, where \mathcal{L} is a linear operator on matrices; formula for $\text{vec}(\mathcal{E})$, where \mathcal{E} is a quantum operation; extracting $\text{vec}(\mathcal{E})$ from experimental data; determining the χ matrix from $\text{vec}(\mathcal{E})$; Shoda's first theorem, giving a representation for additive commutators; Shoda's second theorem, giving a representation for multiplicative commutators.

Summary of main ideas: when dealing with matrix equations, vectorizing them will help with solution; insight into quantum operations can be obtained by using their vectorized form; representation theorems for matrices with trace zero and determinant one.

-
- [1] I. L. Chuang and M. A. Nielsen, *J. Mod. Opt.* **44**, 2455 (1997), arXiv:quant-ph/9610001.
 - [2] J. F. Poyatos, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **78**, 390 (1997).
 - [3] A. Y. Kitaev, *Russ. Math. Surv.* **52**, 1191 (1997).
 - [4] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).
 - [5] R. A. Horn and C. R. Johnson, *Topics in matrix analysis*

- (Cambridge University Press, Cambridge, 1991).
- [6] W. E. Roth, *Bull. Amer. Math. Soc.* **40**, 461 (1934).
- [7] M. B. Ruskai, *Rev. Math. Phys.* **6**, 1147 (1994).
- [8] A. Horn, *Amer. J. Math.* **76**, 620 (1954).
- [9] M. A. Nielsen, *Phys. Rev. A* **62**, 052308 (2000), arXiv:quant-ph/9909020.
- [10] A. W. Marshall and I. Olkin, *Inequalities: theory of majorization and its applications* (Academic Press, New York, 1979).