http://mmg.tversu.ru ISSN 2311-1275

MMG Mathematical Modelling and Geometry

Volume 8, No 3, pp. 1 – 14 (2020) doi:10.26456/mmg/2020-831

Pauli basis formalism in quantum computations

V. V. Nikonov[a] **and A. N. Tsirulev**[b]

Faculty of Mathematics, Tver State University, Sadovyi per. 35, Tver, Russia

e-mail: [a] nikonov.vv@tversu.ru [b] tsirulev.an@tversu.ru

Received 1 December 2020, in final form 28 December. Published 30 December 2020.

Abstract. This article deals with quantum computations in the Pauli basis whose elements are usually identified with the Pauli strings. This approach allows us to represent quantum states, observables, and unitary operators in the unified form of linear combination of Pauli strings, so that all operations can be reduced to the string compositions. Nevertheless a formal justification of the Pauli basis for quantum computations should be based on the strong results of complex linear algebra and the theory of Hilbert spaces. We briefly review the main features of Pauli strings for quantum states and unitary operators, and also the key operations with them, including an algorithm for string compositions and a transformation algorithm from the standard basis to the Pauli basis.

Keywords: quantum computations, Pauli basis

MSC numbers: 81P16, 81P68

1. Introduction

The theory of quantum computing remains in the field of great attention over the past two decades. Various types and subtypes of quantum computations are adapted for different technologies and hardware architectures, but their mathematical structures are constructed using the same basic notions of Hilbert space, quantum observable, unitary operator, and quantum state. In this article, we consider interacting composite quantum system consisting of n identical two-level subsystems (qubits), so that the dimension of the corresponding Hilbert space is 2^n. A pure state quantum computation with a number of gates that polynomially depends on the number of qubits can be efficiently simulated classically. Since a universal quantum computer demonstrating quantum supremacy should have a large number of qubits, say $n \geq 1000$, the number of basis states is $2^n > 10^{300}$. Quantum computers with small number of qubits ($n \sim 100$) that will be available in the near term have to employed together with a classical computer. In both cases multi-qubit quantum computations are very sensitive to the choice of a computational basis [1, 2, 3].

There are two general possibilities for choosing a basis, and which one is more efficient depends on both a given algorithm and a particular type of quantum computer. First, we can use a standard orthonormal basis in the based Hilbert space and then construct a suitable basis in the algebra of linear operators. However, this approach turns out to be inconvenient and unnatural in the consideration of problems related to mixed states, graph states [4], error corrections [3, 5, 6], tensor networks [7, 8, 9] and more generally, to all issues where measurements are not projective [10, 11, 12]. The second possibility deals directly with a basis in the operator algebra, and in this case the basis elements usually cannot be separated into the tensor product of some ket and bra vectors; the Pauli basis is considered to be the best choice because it is Hermitian, orthonormal (with respect to the Hilbert-Schmidt inner product), and makes up an orthonormal basis in the Lie algebra of the corresponding unitary group. The Clifford group, which has numerous applications in quantum computations, is most simply described in terms of the Pauli basis [10, 14].

The main purpose of this article is to give a systematic algebraic overview of multiqubit systems in the Pauli basis. The article is organized as follows. Section 2 contains some necessary mathematical preliminaries. In Section 3 we give a short description of quantum states for a n-qubit quantum system in the Pauli basis. Section 4 is devoted to studying some computational properties of Pauli strings. In Section 5 we consider a computational algorithms intended for transition from the standard basis to the Pauli basis.

Throughout this article, we use the natural units with $\hbar = c = 1$. For the sake of readability, some notations have been made context sensitive: lowercase Latin letters in binary strings (e.g., in symbols of bra and ket) take the values 0 and 1, while in Pauli strings and indices they run from 0 to 3.

2. Main features of the Pauli basis

We will consider a quantum system of n distinguishable qubits, where a qubit is associated with a two-dimensional Hilbert space $\mathcal{H}$ and its dual (Hermitian adjoint) space $\mathcal{H}^\dagger$. Let $\mathcal{H}_n = \mathcal{H}^{\otimes n}$ and $\mathcal{H}_n^\dagger = \left(\mathcal{H}^\dagger\right)^{\otimes n}$ be the Hilbert space of the system and its dual, respectively, and let $L(\mathcal{H}_n) = \mathcal{H}_n \otimes \mathcal{H}_n^\dagger$ be the space of linear operators acting on $\mathcal{H}$ and $\mathcal{H}^\dagger$ by the left and right contractions respectively. Then

$$\dim_{\mathbb{C}}\mathcal{H}_n = \dim_{\mathbb{C}}\mathcal{H}_n^\dagger = 2^n, \quad \dim_{\mathbb{C}} L(\mathcal{H}_n) = 2^{2n}.$$

We will also assume that the space $L(\mathcal{H}_n)$ is equipped with the Hilbert-Schmidt inner product,

$$\langle \hat{A}, \hat{B} \rangle = \operatorname{tr}(\hat{A}^\dagger \hat{B}), \quad \hat{A}, \hat{B} \in L(\mathcal{H}_n), \tag{1}$$

which is the natural extension of the inner product in $\mathcal{H}_n$. The real linear space of Hermitian operators is denoted below as $H(\mathcal{H}_n)$.

Let $\{|0\rangle, |1\rangle\}$ be an orthonormal basis in some one-qubit space $\mathcal{H}$. The unit matrix and the Pauli matrices,

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

define the four Pauli operators

$$\hat{\sigma}_0 = |0\rangle\langle 0| + |1\rangle\langle 1|, \qquad \hat{\sigma}_1 = |0\rangle\langle 1| + |1\rangle\langle 0|,$$

$$\hat{\sigma}_2 = -i|0\rangle\langle 1| + i|1\rangle\langle 0|, \quad \hat{\sigma}_3 = |0\rangle\langle 0| - |1\rangle\langle 1|,$$

which are Hermitian and unitary at the same time, and which form a basis in $L(\mathcal{H})$. The inverse transformation is given by

$$|0\rangle\langle 0| = \frac{\hat{\sigma}_0 + \hat{\sigma}_3}{2}, \quad |0\rangle\langle 1| = \frac{\hat{\sigma}_1 + i\hat{\sigma}_2}{2}, \quad |1\rangle\langle 0| = \frac{\hat{\sigma}_1 - i\hat{\sigma}_2}{2}, \quad |1\rangle\langle 1| = \frac{\hat{\sigma}_0 - \hat{\sigma}_3}{2}.$$

Recall that for $k, l, m \in \{1, 2, 3\}$ we have $\operatorname{tr}\hat{\sigma}_k = 0$, $\hat{\sigma}_k^2 = \hat{\sigma}_0$, and

$$\hat{\sigma}_k\hat{\sigma}_l = -\hat{\sigma}_l\hat{\sigma}_k, \quad \hat{\sigma}_k\hat{\sigma}_l = i\,\operatorname{sign}(\pi)\hat{\sigma}_m, \ \ (klm) = \pi(123), \tag{2}$$

where $\pi(123)$ is a permutation of $\{1, 2, 3\}$.

There is a *standard*[1] binary basis in $\mathcal{H}_n$ generated by the orthonormal bases $\{|0\rangle, |1\rangle\}$ in the corresponding one-qubit spaces. Mathematically, the position in the tensor product distinguishes qubits from each other. Therefore, for a fixed n, it is convenient to write an element of this basis and the corresponding element of the dual basis in the form

$$|k\rangle = |k_1 \dots k_n\rangle = |k_1\rangle \otimes \dots \otimes |k_n\rangle, \quad \langle k| = \langle k_1 \dots k_n| = \langle k_1| \otimes \dots \otimes \langle k_n|,$$

[1] We do not use the usual term "computational" because it can lead to confusion. The Pauli basis and the standard basis are computational in the same sense.

regarding the strings $k_1 \dots k_n$ ($k_1, \dots, k_n \in \{0,1\}$) as a binary number and denoting it by its decimal representation k. For example, $|101\rangle = |5\rangle$ and $|00110\rangle = |6\rangle$

In the standard basis,

$$|u\rangle = \sum_{k=0}^{2^n-1} u_k |k\rangle, \quad \hat{A} = \sum_{k,l=0}^{2^n-1} a_{kl} |k\rangle\langle l|,$$

where $|u\rangle \in \mathcal{H}_n$ and $\hat{A} \in L(\mathcal{H}_n)$.

The *Pauli basis* $P(\mathcal{H}_n)$ in $L(\mathcal{H}_n)$ is defined by

$$\left\{\hat{\sigma}_{k_1 \dots k_n}\right\}_{k_1,\dots,k_n \in \{0,1,2,3\}}, \qquad \hat{\sigma}_{k_1\dots k_n} = \hat{\sigma}_{k_1} \otimes \dots \otimes \hat{\sigma}_{k_n}, \tag{3}$$

where $\hat{\sigma}_{0\dots 0}$ is the identity operator. It is obvious that the $P(\mathcal{H}_n)$ consists of 4^n elements. We will use compact notations like

$$\hat{\sigma}_K = \hat{\sigma}_{k_1\dots k_n},$$

denoting the *Pauli string* $k_1 \dots k_n$, where $k_1, \dots, k_n \in \{0,1,2,3\}$, by the corresponding capital letter K. In doing so, we will often consider K as a number, that is, as the decimal representation of the string; it is clear that $0 \leqslant K \leqslant 4^n - 1$. Note that the Pauli string K and the element $\hat{\sigma}_K$ of the Pauli basis are completely determined by each other and, consequently, can be identified. For example, elements of the standard basis are expressed in terms of the Pauli basis in Appendix A1 on page 12.

It is useful to compare $P(\mathcal{H}_n)$ with the standard basis. We have

$$\hat{\sigma}_{k_1\dots k_n}\hat{\sigma}_{k_1\dots k_n} = \hat{\sigma}_{0\dots 0}, \quad \operatorname{tr}\hat{\sigma}_{0\dots 0} = 2^n, \quad \operatorname{tr}\hat{\sigma}_{k_1\dots k_n}\big|_{k_1\dots k_n \neq 0\dots 0} = 0. \tag{4}$$

The Pauli basis is Hermitian, unitary, and orthogonal with respect to the inner product (1). Note that the operator $|k\rangle\langle l|$ of the standard basis is not unitary, and it is not Hermitian if $k \neq l$. The standard basis does not contain the identity operator which has the form

$$\sum_{k=0}^{2^n-1} |k\rangle\langle k|$$

in that basis. In the Pauli basis, any operator $\hat{U}$ from the unitary group $U(\mathcal{H}_n)$ (that is, $\hat{U}^\dagger\hat{U} = \hat{\sigma}_{0\dots 0}$) has an expansion of the form

$$\hat{U} = \sum_{i_1,\dots,i_n \in \{0,1,2,3\}} U_{i_1\dots i_n}\hat{\sigma}_{i_1\dots i_n}, \quad \hat{U}^\dagger = \sum_{i_1,\dots,i_n \in \{0,1,2,3\}} \overline{U}_{i_1\dots i_n}\hat{\sigma}_{i_1\dots i_n},$$

where

$$\sum_{i_1,\dots,i_n \in \{0,1,2,3\}} \overline{U}_{i_1\dots i_n} U_{i_1\dots i_n} = 1, \qquad \sum_{\substack{i_1,\dots,i_n,\, j_1,\dots,j_n \in \{0,1,2,3\} \\ (i_1,\dots,i_n) \neq (j_1,\dots,j_n)}} \overline{U}_{i_1\dots i_n} U_{j_1\dots j_n} = 0.$$

Note that the letter condition can be obviously decomposed into $2^{2n-1}\big(2^n - 1\big)$ independent conditions.

3. Quantum states in the Pauli basis

A quantum state (a density operator) is a Hermitian, positive semidefinite (or positive[1], in short) operator of the form

$$\hat{\rho} = \frac{1}{2^n} \sum_{k_1,\ldots,k_n \in \{0,1,2,3\}} a_{k_1\ldots k_n} \hat{\sigma}_{k_1\ldots k_n} \equiv \frac{1}{2^n} \sum_{K=0}^{4^n-1} a_K \hat{\sigma}_K, \tag{5}$$

where $a_{k_1\ldots k_n} \in \mathbb{R}$ and

$$a_{0\ldots 0} = 1\,, \quad |a_{k_1\ldots k_n}| \leqslant 1, \qquad \sum_{k_1,\ldots,k_n \in \{0,1,2,3\}} (a_{k_1\ldots k_n})^2 \leqslant 2^n. \tag{6}$$

The conditions (6) guarantee that $\hat{\rho}^\dagger = \hat{\rho}$, $\operatorname{tr}\hat{\rho} = 1$, and $\operatorname{tr}\hat{\rho}^2 \leqslant 1$. For quantum computation, it is important that all coefficients in the state (5) are real and each of them, except $a_{0\ldots0}$, is exactly the result of a local measurement with one of the basis operators (3), $a_K \equiv a_{k_1\ldots k_n} = \operatorname{tr}\big(\hat{\rho}\hat{\sigma}_{k_1\ldots k_n}\big)$. All the quantum (pure and mixed) states constitute a convex set (closed manifold, since it is the preimage of 1 under the map $\operatorname{tr}: H(\mathcal{H}_n) \to \mathbb{R}$) of real dimension $4^n - 1$ in the real linear manifold $\mathcal{S}_n \subset \operatorname{Span}\{P(\mathcal{H}_n)\} = H(\mathcal{H}_n)$, while the pure states are placed on the boundary of $\mathcal{S}_n$ and make up a real submanifold of dimension $2^{n+1} - 2$.

Each element of $P(\mathcal{H}_n)$ is idempotent ($\hat{\sigma}_K\hat{\sigma}_K = \hat{\sigma}_{0\ldots0}$), so that the operators

$$\hat{P}_K^{\pm} = \frac{\hat{\sigma}_{0\ldots0} \pm \hat{\sigma}_K}{2}$$

are projectors. Thus, the observable $\hat{\sigma}_K = \hat{P}^+ - \hat{P}^-\ \hat{\sigma}_K$ is naturally reduced to projective measurements. Using the operators $\hat{P}_K^{\pm}$, we can now prove the following practically important proposition which seems to have not been considered in, at least, the current literature.

Proposition 1. *The condition $|a_{k_1\ldots k_n}| \leqslant 1$ in (6) follows from the positive definiteness of the density operator (5) and the first condition in (6).*

Note that Hermitian projectors $\hat{P}_K^{\pm} = \hat{P}_K^{\pm}\hat{P}_K^{\pm} = \big(\hat{P}_K^{\pm}\big)^\dagger \hat{P}_K^{\pm}$ are positive operators because of the obvious inequalities

$$\langle u|\hat{P}_K^{\pm}|u\rangle = \langle u|\big(\hat{P}_K^{\pm}\big)^\dagger \hat{P}_K^{\pm}|u\rangle \geqslant 0.$$

In general a Hermitian operator $\hat{A} \in L(\mathcal{H}_n)$ is positive if and only if there exists some operator $\hat{B} \in L(\mathcal{H}_n)$ such that $\hat{A} = \hat{B}\hat{B}^\dagger$; moreover, $\hat{B}$ can be chosen to be Hermitian [15]. It in turn implies that ($\hat{A}$ and $\hat{\rho}$ are positive)

$$\operatorname{tr}\big(\hat{A}\hat{\rho}\big) = \operatorname{tr}\big(\hat{B}\hat{B}^\dagger\hat{\rho}\big) = \operatorname{tr}\big(\hat{B}^\dagger\hat{\rho}\hat{B}\big) \geqslant 0,$$

[1] For our purpose in this article, we do not need to distinguish between positive semidefinite and positive definite operators.

since $\hat{B}^\dagger\hat{\rho}\hat{B}$ is obviously positive. Thus,

$$\mathrm{tr}\big(\hat{P}_K^{\pm}\hat{\rho}\big) = \frac{1 \pm a_K}{2} \geqslant 0, \tag{7}$$

so that $-1 \leqslant a_K \leqslant 1$. The proof is complete. □

As an example, we write down one of the practically useful states in the standard basis and in the Pauli basis, namely, the three-qubit Greenberger-Horne-Zeilinger state. Using the operator $CNOT$ and the Hadamard operator $\hat{U}_2^+$, which are defined by relations (13) and (14) in Appendix A2, we can write the unitary transformation of the initial state $|000\rangle$ to the GHZ_3 state in the form

$$\hat{U}_{\mathrm{GHZ}_3} = \big(\hat{\sigma}_0 \otimes CNOT\big)\circ\big(CNOT \otimes \hat{\sigma}_0\big)\circ\big(\hat{U}_2^+ \otimes \hat{\sigma}_{00}\big),$$

from which it is easy to find

$$\begin{aligned}\hat{\rho}_{\mathrm{GHZ}_3} = &= \frac{1}{2}\big(|000\rangle\langle 000| + |000\rangle\langle 111| + |111\rangle\langle 000| + |111\rangle\langle 111|\big)\\ &= \frac{1}{8}\big(\hat{\sigma}_{000} + \hat{\sigma}_{111} - \hat{\sigma}_{122} - \hat{\sigma}_{212} - \hat{\sigma}_{221} + \hat{\sigma}_{033} + \hat{\sigma}_{303} + \hat{\sigma}_{330}\big).\end{aligned}$$

4. Operations with Pauli strings

We will need a few facts and definitions related to the Pauli basis and to the set of n-length Pauli strings,

$$\mathrm{Str}_n = \{K = k_1 \ldots k_n\}_{k_1,\ldots,k_n \in \{0,1,2,3\}}.$$

First, let us consider the set $\mathbb{F}_4 = \{0,1,2,3\}$ as the Klein four-group with the multiplication rules

$$0{*}k = k, \quad k{*}k = 0, \quad k{*}l = m,$$

where $k,l,m \in \{1,2,3\}$ and klm is any permutation of 123. Second, let the function $s : \mathbb{F}_4 \times \mathbb{F}_4 \to \{1, i, -i\}$ be defined by its values

$$\begin{aligned}&s(0,0) = s(0,k) = s(k,0) = s(k,k) = 1, \quad k = 1,2,3,\\ &s(1,2) = s(2,3) = s(3,1) = i, \quad s(2,1) = s(3,2) = s(1,3) = -i.\end{aligned}$$

Further, let the function $S : \mathrm{Str}_n \times \mathrm{Str}_n \to \{1,-1,i,-i\}$, $(K,L) \mapsto S_{KL}$, be defined as the product

$$S_{KL} = s(k_1,l_1)s(k_2,l_2)\ldots s(k_n,l_n), \quad K = k_1k_2\ldots k_n, \;\; L = l_1l_2\ldots l_n.$$

The function S is symmetric or antisymmetric depending on the number of pairs (k_r, l_r) (r is a position in the strings K and L) such that $k_r, l_r \in \{1,2,3\}$ and $k_r \neq l_r$, and also depending on the relative ordering in them. Let w_{KL}^+ and w_{KL}^- be the numbers of pairs of the forms $(1,2),(2,3),(3,1)$ and of the forms $(2,1),(3,2),(1,3)$ respectively, and let $w_{KL} = w^+_{KL} + w^-_{KL}$. Then

$$S_{KL} = (i)^{w_{KL}}(-1)^{w^-_{KL}}, \quad S_{(KL)} = \frac{S_{KL}}{2}\big(1+(-1)^{w_{KL}}\big), \quad S_{[KL]} = \frac{S_{KL}}{2}\big(1-(-1)^{w_{KL}}\big), \tag{8}$$

where round and square brackets denote symmetrization and antisymmetrization, respectively. The values of S_{KL}, $S_{(KL)}$, and $S_{[KL]}$ are given in Table 2.

$w_{KL} \bmod 4$	0	2	0	2	1	3	1	3
$w^-_{KL} \bmod 2$	0	1	1	0	0	1	1	0
S_{KL}	1	1	-1	-1	i	i	$-i$	$-i$
$S_{(KL)}$	1	1	-1	-1	0	0	0	0
$S_{[KL]}$	0	0	0	0	i	i	$-i$	$-i$

Table 1: The factors before $\hat\sigma_M$ in (9) for $\hat\sigma_K\hat\sigma_L$, $\{\hat\sigma_K, \hat\sigma_L\}$, and $[i\hat\sigma_K, i\hat\sigma_L]$.

Now the composition of two Pauli basis elements and their anticommutator and commutator can be written in the form of compact expressions that are convenient for classical computer programming:

$$\hat\sigma_K\hat\sigma_L = S_{KL}\hat\sigma_M, \quad \{\hat\sigma_K, \hat\sigma_L\} = S_{(KL)}\hat\sigma_M, \quad [i\hat\sigma_K, i\hat\sigma_L] = -S_{[KL]}\hat\sigma_M, \tag{9}$$

where

$$\hat\sigma_M = \hat\sigma_{m_1\ldots m_n}, \quad m_1 = k_1{*}l_1, \ \ldots, m_n = k_n{*}l_n. \tag{10}$$

Note that two Pauli strings of length n can commute, even if they have different nonzero entries in some the same locations. For example, the three operators $\hat\sigma_{11}$, $\hat\sigma_{22}$, and $\hat\sigma_{33}$ mutually commute. It is also easy to see that the unitary transition matrix, transforming the standard basis $\big\{|i_1 \ldots i_n\rangle\langle j_1 \ldots j_n|\big\}$ into the Pauli basis, consists of only the elements 0, ± 1, and $\pm i$. In particular,

$$|00\ldots0\rangle\langle 00\ldots0| \to \frac{1}{2^n}\sum_{i_1,\ldots,i_n\in\{0,3\}} \hat\sigma_{i_1\ldots i_n}.$$

More generally, the standard orthogonal projectors can be expressed as

$$|i_1\ldots i_n\rangle\langle i_1\ldots i_n|_{i_1,\ldots,i_n\in\{0,1\}} = \frac{1}{2^n}\sum_{k_1,\ldots,k_n\in\{0,3\}} \chi^{i_1}_{k_1}\cdots\chi^{i_n}_{k_n}\,\hat\sigma_{k_1\ldots k_n},$$

where

$$\chi^0_0 = \chi^0_3 = \chi^1_0 = 1, \quad \chi^1_3 = -1.$$

Some important operators in the Pauli basis are written in Appendix A2 on page 14.

The expressions (9) show, first, that the set $\{i\hat{\sigma}_K\}_{K=0}^{4^n-1}$ makes up an orthonormal basis in $\mathfrak{su}(n)$. And, second, the set

$$\widetilde{P}(\mathcal{H}_n) = \bigl\{\epsilon\hat{\sigma}_K \,|\, K \in \mathrm{Str}_n,\ \epsilon \in \{\pm 1,\ \pm i\}\bigr\},$$

which consists of 4^{n+1} elements, is a group; it is called the (n-qubit) Pauli group. The normalizer of the Pauli group,

$$\mathcal{C}(\mathcal{H}_n) = \bigl\{\hat{U} \in U(\mathcal{H}_n) \mid \hat{U}\hat{\sigma}_K\hat{U}^\dagger \in \widetilde{P}(\mathcal{H}_n),\ \hat{\sigma}_K \in \widetilde{P}(\mathcal{H}_n)\bigr\},$$

is called the Clifford group. We have from 2, 4, and 10 the following proposition:

Proposition 2. *The mutual unitary transformations of the Pauli basis operators obey the relations* $\hat{\sigma}_{i_1\ldots i_n}\hat{\sigma}_{k_1\ldots k_n}\hat{\sigma}_{i_1\ldots i_n} = \pm\hat{\sigma}_{i_1\ldots i_n}$*, where the plus sign takes place if and only if the number of triples* $(i_m k_m i_m)_{m\in\{1,\ldots,n\}}$*, satisfying the conditions* $i_m \neq k_m$*,* $i_m \neq 0$*, and* $k_m \neq 0$*, is even.*

5. Algorithms for transition to the Pauli basis

In a standard basis and in the Pauli basis, we can express an operator $\hat{A} \in L(\mathcal{H}_n)$ (for example, a unitary transformation, an observable, or a density operator) as

$$\hat{A} = \sum_{i_0,\ldots,i_{n-1},j_0,\ldots,j_{n-1}\in\{0,1\}} a_{i_{n-1}\ldots i_0 j_{n-1}\ldots j_0} |i_{n-1}\ldots i_0\rangle\langle j_{n-1}\ldots j_0| \\ = \frac{1}{2^n}\sum_{i_0,\ldots,i_{n-1}\in\{0,1,2,3\}} s_{i_{n-1}\ldots i_0}\hat{\sigma}_{i_{n-1}\ldots i_0},$$

or, in short,

$$\hat{A} \;=\; \sum_{i=0}^{2^n-1}\sum_{j=0}^{2^n-1} a_{ij}|i\rangle\langle j| \;=\; \frac{1}{2^n}\sum_{I=0}^{4^n-1} S_I\hat{\sigma}_I. \tag{11}$$

Thus, we deal with the problem of calculating the coefficients S_I when the coefficients a_i are given; such an algorithm have recently been proposed [13]. Our approach is based on the following observation: all coefficients a_{ij} with binary strings $i = i_{n-1}\ldots i_0$ and $j = j_{n-1}\ldots j_0$, which have the same sum

$$k \;=\; (k_{n-1}\ldots k_0)_2 \;=\; (i_{n-1}\ldots i_0)_2 \oplus (j_{n-1}\ldots j_0)_2\,,$$

give nonzero contributions only to the terms of the form $S_l^{(i\oplus j)}\hat{\sigma}_l$, where l is a binary string $l_{n-1}\ldots i_0$, $0 \leqslant l \leqslant 2^n-1$, and the operators $\hat{\sigma}_l$ must be recalculated to the form (11). It is straightforward (but cumbersome) to prove that the strings $I = I(k,l) = \bigl[I_0^{(k)},\ldots,I_{2^n-1}^{(k)}\bigr]_4$, $k = i\oplus j$, in $\hat{\sigma}_I$ are determined by

$$I = \bar{l}\wedge k + 2\bigl(l\wedge k\bigr) + 3\bigl(l\wedge\bar{k}\bigr), \tag{12}$$

where a bar above a letter denotes the inversion $0 \leftrightarrow 1$ for each digit of the corresponding binary string, and $\wedge$ denotes the logical operation OR. On the right hand side in (12), we consider the resulting binary strings as base-4 numbers. For given binary strings i and j, the pseudocode of this procedure is written in Algorithm 1.

For example, summands

$$a_{010,001}|010\rangle\langle 001| = \frac{a_{21}}{2^3}\big(\hat\sigma_{011} + i\hat\sigma_{012} - i\hat\sigma_{021} + \hat\sigma_{022} + \hat\sigma_{311} + i\hat\sigma_{312} - i\hat\sigma_{321} + \hat\sigma_{322}\big),$$

$$a_{001,010}|001\rangle\langle 010| = \frac{a_{12}}{2^3}\big(\hat\sigma_{011} - i\hat\sigma_{012} + i\hat\sigma_{021} + \hat\sigma_{022} + \hat\sigma_{311} - i\hat\sigma_{312} + i\hat\sigma_{321} + \hat\sigma_{322}\big),$$

$$a_{101,110}|101\rangle\langle 110| = \frac{a_{56}}{2^3}\big(\hat\sigma_{011} - i\hat\sigma_{012} + i\hat\sigma_{021} + \hat\sigma_{022} - \hat\sigma_{311} + i\hat\sigma_{312} - i\hat\sigma_{321} - \hat\sigma_{322}\big),$$

$$a_{111,100}|111\rangle\langle 100| = \frac{a_{74}}{2^3}\big(\hat\sigma_{011} - i\hat\sigma_{012} - i\hat\sigma_{021} - \hat\sigma_{022} - \hat\sigma_{311} + i\hat\sigma_{312} + i\hat\sigma_{321} + \hat\sigma_{322}\big)$$

will contribute to the linear combination of $\hat\sigma_{011}$, $\hat\sigma_{012}$, $\hat\sigma_{021}$, $\hat\sigma_{022}$, $\hat\sigma_{311}$, $\hat\sigma_{312}$, $\hat\sigma_{321}$, and $\hat\sigma_{322}$ with

$$k = 010 \oplus 001 = 001 \oplus 010 = 101 \oplus 110 = 111 \oplus 100 = \mathbf{011}.$$

The elements of the Pauli basis emerging in (12) from these summands are shown in Table 2. For example, if $l = 5 = (101)_2$, then, in accordance with (12),

$$\begin{aligned} I^{(3)}[5] = \big[(010)_2 \wedge (011)_2\big]_4 + 2\big[(101)_2 \wedge (011)_2\big]_4 + 3\big[(101)_2 \wedge (100)_2\big]_4 \\ = \big[010\big]_4 + 2\big[001\big]_4 + 3\big[100\big]_4 = 312. \end{aligned}$$

Next, as an example, the summand $a_{101,110}|101\rangle\langle 110| = a_{56}|5\rangle\langle 6|$ contributes $ia_{56}/2^3$ in $S^{(3)}[5]$, since there are the triples $(l_0 i_0 j_0) = (110)_2$, $(l_1 i_1 j_1) = (001)_2$, and $(l_2 i_2 j_2) = (111)_2$ in Algorithm 1 (lines 17 – 26); therefore, $sign = 1$, $c = 1$.

l	0	1	2	3	4	5	6	7
$l_2 l_1 l_0$	000	001	010	011	100	101	110	111
$k_2 k_1 k_0$	011	011	011	011	011	011	011	011
$\bar l \wedge k$	011	010	001	000	011	010	001	000
$l \wedge k$	000	001	010	011	000	001	010	011
$l \wedge \bar k$	000	000	000	000	100	100	100	100
$\hat\sigma_I$	$\hat\sigma_{011}$	$\hat\sigma_{012}$	$\hat\sigma_{021}$	$\hat\sigma_{022}$	$\hat\sigma_{311}$	$\hat\sigma_{312}$	$\hat\sigma_{321}$	$\hat\sigma_{322}$

Table 2: The elements of the Pauli basis emerging for $k = 011$.

Algorithm 1 Transformation to the Pauli basis.

Input the number of qubits n
Input strings $i = i_{n-1} \dots i_0$ and $j = j_{n-1} \dots j_0$, $i_s, j_s \in \{0, 1\}$
Input a complex number a_{ij} — the factor in $a_{ij}|i\rangle\langle j|$
//Make up the row number $k = i \oplus j$
Initialize string $k = \text{null}$
for $i_s = i_0, \dots, i_{n-1}$ **do**
  for $j_s = j_0, \dots, j_{n-1}$ **do**
    $k_s = i_s \oplus j_s$
  end for
end for
Convert $(k_{n-1} \dots k_0)_2$ to int $(k)_{10}$
//For the number k*, fill in two rows*
Initialize $S^{(k)}$ by zero 2^n-length complex-data-type vector
Initialize $I^{(k)}$ by null 2^n-length string-data-type vector
Initialize int $cntr$ and $sign \in \{1, -1, i, -i\}$ by arbitrary values
for $l = 0$ **to** $2^n - 1$ **do**
  Convert $(l)_{10}$ to $(l_{n-1} \dots l_0)_2$
  $cntr = 0$ and $sign = 1$
  for $l_s = l_0, \dots, l_{n-1}$ **do**
    if $l_s == 1$ **then**
      if $(i_s, j_s) == (1, 1)$ **then** $sign = -sign$
      if $(i_s, j_s) == (0, 1)$ **then** $cntr = cntr + 1$
      if $(i_s, j_s) == (1, 0)$ **then** $sign = -sign$, $cntr = cntr + 1$
    end if
  end for
  $I^{(k)}[l] = \bar{l} \wedge k + 2\big(l \wedge k\big) + 3\big(l \wedge \bar{k}\big)$
  int $c = cntr \ (mod 4)$, $S^{(k)}[l] += i^c \cdot sign \cdot a_{ij}$
end for
Return the rows $S^{(k)}$ and $I^{(k)}$.

6. Conclusion

In this article, we have described a base technique for working with the Pauli basis. It is shown that this technique can make more convenient and algorithmic some manipulations with mathematical expressions related to quantum circuits with large number of qubits. We have presented a new efficient algorithm with a polynomial complexity for transition from the standard basis to the Pauli basis.

References

[1] B. Dirkse, M. Pompili, R. Hanson, M. Walter, S. Wehner *Witnessing Entanglement in Experiments with Arbitrary Noise* Quantum Science and Technology **5**, 035007, 2020 (arXiv:1909.09119)

[2] I. Hamamura and T. Imamichi *Efficient evaluation of quantum observables using entangled measurements* npj Quantum Information **6**, 56, 2020 (arXiv:1909.09119)

[3] O. Crawford, B. van Straaten, D. Wang, T. Parks, E. Campbell, S. Brierley *Efficient quantum measurement of Pauli operators in the presence of finite sampling error* Quantum **5**, 385–404, 2021 (arXiv:1908.06942)

[4] W. Klobus et al. *Higher dimensional entanglement without correlations.* Eur. Phys. J. D **73**, 29, 2019 (arXiv:1808.10201)

[5] T.J. O'Connor, Y. Yu, B. Helou, R. Laflamme *The robustness of magic state distillation against errors in Clifford gates* Quantum Information & Computation **13**, 361–378, 2013 (arXiv:1205.6715)

[6] C.A. Riofrio, D. Gross, S.T. Flammia, T. Monz, D. Nigg, R. Blatt, J. Eisert *Experimental quantum compressed sensing for a seven-qubit system* Nature Comm. **8**, 15305, 2017 (arXiv:1608.02263)

[7] S.S. Jahromi, R. Orus *A universal tensor network algorithm for any infinite lattice* Phys. Rev. D **99**, 195105, 2019 (arXiv:1808.00680)

[8] A.N. Tsirulev *A geometric view on quantum tensor networks* Europ. Phys. J. Web of Conferences **226**, No 4, 2020 (`https://doi.org/10.1051/epjconf/202022602022`)

[9] I.M. Potashov, A.N. Tsirulev *Computational Algorithm for Covariant Series Expansions in General Relativity* Europ. Phys. J. Web of Conferences **173**, 03021, 2018 (`https://doi.org/10.1051/epjconf/201817303021`)

[10] S. Bravyi and A. Kitaev *Universal quantum computation with ideal Clifford gates and noisy ancillas* Phys. Rev. A **71**, 022316, 2005 (arXiv:quant-ph/0403025)

[11] V. Danos and E. Kashefi *Determinism in the one-way model* Phys. Rev. A. **74**, 052310, 2006 (arXiv:quant-ph/0506062)

[12] V. Danos and E. Kashefi *Pauli measurements are universal* Electronic Notes in Theoretical Computer Science **170**, 95–100, 2007 (`https://doi.org/10.1016/j.entcs.2006.12.013`)

[13] D. Gunlycke, M.C. Palenik, and S.A. Fischer *Efficient algorithm for generating Pauli coordinates for an arbitrary linear operator* 2020 (arXiv:2011.08942)

[14] S. Bravyi and D. Maslov *Hadamard-free circuits expose the structure of the Clifford group.* 2020 (arXiv: 2003.09412)

[15] I. Bengtsson, K. Zyczkowski *Geometry of Quantum States: An Introduction to Quantum Entanglement.* Cambridge University Press, Cambridge, 2006

[16] V.V. Shende, I.L. Markov, and S.S. Bullock *Minimal universal twoqubit controlled-NOT-based circuits* Phys. Rev. A, **69**, 062321, 2004 (arXiv:quant-ph/0308033)

Appendix

A1. The Pauli basis for $n = 2$

For reference, we give here expressions of the elements of the standard basis in $\mathcal{H}_2$ in terms of the elements of the Pauli basis. Recall that such expressions in $\mathcal{H}_1$ have the form

$$|0\rangle\langle 0| = \frac{\hat\sigma_0 + \hat\sigma_3}{2}\,, \quad |0\rangle\langle 1| = \frac{\hat\sigma_1 + i\hat\sigma_2}{2}\,, \quad |1\rangle\langle 0| = \frac{\hat\sigma_1 - i\hat\sigma_2}{2}\,, \quad |1\rangle\langle 1| = \frac{\hat\sigma_0 - \hat\sigma_3}{2}\,.$$

$$|00\rangle\langle 00| = \frac{\hat\sigma_{00} + \hat\sigma_{03} + \hat\sigma_{30} + \hat\sigma_{33}}{4}\,, \qquad |01\rangle\langle 00| = \frac{\hat\sigma_{01} - i\hat\sigma_{02} + \hat\sigma_{31} - i\hat\sigma_{32}}{4}\,,$$

$$|10\rangle\langle 00| = \frac{\hat\sigma_{10} + \hat\sigma_{13} - i\hat\sigma_{20} - i\hat\sigma_{23}}{4}\,, \qquad |11\rangle\langle 00| = \frac{\hat\sigma_{11} - i\hat\sigma_{12} - i\hat\sigma_{21} - \hat\sigma_{22}}{4}\,,$$

$$|00\rangle\langle 01| = \frac{\hat\sigma_{01} + i\hat\sigma_{02} + \hat\sigma_{31} + i\hat\sigma_{32}}{4}\,, \qquad |01\rangle\langle 01| = \frac{\hat\sigma_{00} - \hat\sigma_{03} + \hat\sigma_{30} - \hat\sigma_{33}}{4}\,,$$

$$|10\rangle\langle 01| = \frac{\hat\sigma_{11} + i\hat\sigma_{12} - i\hat\sigma_{21} + \hat\sigma_{22}}{4}\,, \qquad |11\rangle\langle 01| = \frac{\hat\sigma_{10} - \hat\sigma_{13} - i\hat\sigma_{20} + i\hat\sigma_{23}}{4}\,,$$

$$|00\rangle\langle 10| = \frac{\hat\sigma_{10} + \hat\sigma_{13} + i\hat\sigma_{20} + i\hat\sigma_{23}}{4}\,, \qquad |01\rangle\langle 10| = \frac{\hat\sigma_{11} - i\hat\sigma_{12} + i\hat\sigma_{21} + \hat\sigma_{22}}{4}\,,$$

$$|10\rangle\langle 10| = \frac{\hat\sigma_{00} + \hat\sigma_{03} - \hat\sigma_{30} - \hat\sigma_{33}}{4}\,, \qquad |11\rangle\langle 10| = \frac{\hat\sigma_{01} - i\hat\sigma_{02} - \hat\sigma_{31} + i\hat\sigma_{32}}{4}\,,$$

$$|00\rangle\langle 11| = \frac{\hat\sigma_{11} + i\hat\sigma_{12} + i\hat\sigma_{21} - \hat\sigma_{22}}{4}, \qquad |01\rangle\langle 11| = \frac{\hat\sigma_{10} - \hat\sigma_{13} + i\hat\sigma_{20} - i\hat\sigma_{23}}{4},$$
$$|10\rangle\langle 11| = \frac{\hat\sigma_{01} + i\hat\sigma_{02} - \hat\sigma_{31} - i\hat\sigma_{32}}{4}, \qquad |11\rangle\langle 11| = \frac{\hat\sigma_{00} - \hat\sigma_{03} - \hat\sigma_{30} + \hat\sigma_{33}}{4}.$$

A2. Some unitary operators in the Pauli basis

The controlled-NOT operator:

$$CNOT = \frac{\hat\sigma_{00} + \hat\sigma_{01} + \hat\sigma_{30} - \hat\sigma_{31}}{2} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|, \quad (13)$$

The controlled-phase operator:

$$CZ = \frac{\hat\sigma_{00} + \hat\sigma_{03} + \hat\sigma_{30} - \hat\sigma_{33}}{2} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|.$$

It is well known that $CNOT$ and CZ belong to the Clifford group $\mathcal{C}(\mathcal{H}_2)$. It is also known some sets of generators and canonical forms for operators of the group $\mathcal{C}(\mathcal{H}_n)$ (see, e.g., [14]), but the number of elements in these groups grows exponentially (in fact, slightly faster) with the growth of n: for example, $\mathcal{C}(\mathcal{H}_1)$ is of order 24, and $\mathcal{C}(\mathcal{H}_2)$ is of order 11520. Therefore, there is the problem of finding a practically suitable [16] set of unitary operators for building the Clifford groups and the corresponding stabilizer formalism. Here we introduce the one-qubit Hadamard operator $\hat U_2^+$, and pseudo-Hadamard operators $\hat U_2^-$, $\hat U_1^\pm$ and $\hat U_3^\pm$, obeying the relations $\big(\hat U_1^\pm\big)^2 = \big(\hat U_2^\pm\big)^2 = \big(\hat U_3^\pm\big)^2 = \hat\sigma_0$. They are unitary and Hermitian, and are defined by

$$\begin{aligned}
\hat U_1^\pm &= \frac{\hat\sigma_2 \pm \hat\sigma_3}{\sqrt2} = \frac{1}{\sqrt2}\big(\pm|0\rangle\langle 0| - i|0\rangle\langle 1| + i|1\rangle\langle 0| \mp |1\rangle\langle 1|\big),\\
\hat U_2^\pm &= \frac{\hat\sigma_1 \pm \hat\sigma_3}{\sqrt2} = \frac{1}{\sqrt2}\big(\pm|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| \mp |1\rangle\langle 1|\big), \qquad (14)\\
\hat U_3^\pm &= \frac{\hat\sigma_1 \pm \hat\sigma_2}{\sqrt2} = \mathrm{e}^{\mp i\pi/4}|0\rangle\langle 1| \pm \mathrm{e}^{\pm i\pi/4}|1\rangle\langle 0|.
\end{aligned}$$

They can be used for constructing unitary transformations $\hat\sigma_i \leftrightarrow \pm\hat\sigma_j$ $(i \neq j)$ and $\hat\sigma_i \to -\hat\sigma_i$ $(i = 1,2,3)$:

$$\hat U_k^\pm \hat\sigma_i \hat U_k^\pm = \pm\hat\sigma_j, \quad \hat U_k^\pm \hat\sigma_k \hat U_k^\pm = -\hat\sigma_k, \quad i \neq j \neq k,\ i,j,k \in \{1,2,3\},$$

or, in more detail,

$$\begin{aligned}
\hat U_1^\pm \hat\sigma_2 \hat U_1^\pm &= \pm\hat\sigma_3, & \hat U_1^\pm \hat\sigma_3 \hat U_1^\pm &= \pm\hat\sigma_2, & \hat U_1^\pm \hat\sigma_1 \hat U_1^\pm &= -\hat\sigma_1,\\
\hat U_2^\pm \hat\sigma_1 \hat U_2^\pm &= \pm\hat\sigma_3, & \hat U_2^\pm \hat\sigma_3 \hat U_2^\pm &= \pm\hat\sigma_1, & \hat U_2^\pm \hat\sigma_2 \hat U_2^\pm &= -\hat\sigma_2,\\
\hat U_3^\pm \hat\sigma_1 \hat U_3^\pm &= \pm\hat\sigma_2, & \hat U_3^\pm \hat\sigma_2 \hat U_3^\pm &= \pm\hat\sigma_1, & \hat U_3^\pm \hat\sigma_3 \hat U_3^\pm &= -\hat\sigma_3.
\end{aligned}$$

Further, for the sake of uniformity, we denote $\hat{\sigma}_0$ by $\hat{U}_0$. Thus, for example, we can choose the full set of generators for $\mathcal{C}(\mathcal{H}_1)$ in the form ($\hat{U}_i \equiv \hat{U}_i^+$, $i = 1, 2, 3$)

$$\{\hat{U}_0,\, \hat{U}_1,\, \hat{U}_2,\, \hat{U}_3\}.$$

In the general case of $\widetilde{P}(\mathcal{H}_n)$, a a full set of generators for the group $\mathcal{C}(\mathcal{H}_n)$ constitute operators of the form

$$\{\hat{U}_{i_1 \dots i_n} \;=\; \hat{U}_{i_1} \otimes \cdots \otimes \hat{U}_{i_n}\}_{i_1, \dots, i_n \in \{0,1,2,3\}}.$$