Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

ARTICLE TYPE

An explanation of the Bernstein-Vazirani and Deustch-Josza algorithms with the quantum stabilizer formalism

Elías F. Combarro*[1] | Alejandro Piñera-Nicolás[2] | José Ranilla[1] | Ignacio F. Rúa[2]

[1]Computer Science Department, University of Oviedo, Asturias, Spain
[2]Mathematics Department, University of Oviedo, Asturias, Spain

Correspondence
*Elías F. Combarro Email: efernandezca@uniovi.es

Summary

The standard description of a quantum algorithm consists in three steps. First, encoding the data in a suitable initial quantum state. Second, driving such a state by a convenient sequence of unitary transformations until a final quantum state is reached. Third, measuring the final state and use such a measurement to solve the problem the quantum algorithm was designed for. An alternative description is provided by the stabilizer formalism, that was originally introduced in connection with quantum error correcting codes. In this paradigm, the focus is on the subgroup of elements of the Pauli group stabilizing the initial quantum state, and the transformations that such a subgroup experiments along the algorithm. In this work, we provide an explanation of two foundational quantum algorithms (Bernstein-Vazinari and Deustch-Josza) based on such a quantum stabilizer formalism. Doing so, we provide a better understanding and insight into both procedures which yield to see Bernstein-Vazirani as a particular case of Deustch-Josza, and to introduce a generalized version of Deustch-Josza algorithm.

KEYWORDS:
Quantum Computing, Stabilizer Formalism, Bernstein-Vazarin, Deutsch-Josza, Quantum Error Correcting Codes

1 | INTRODUCTION

The standard description of a quantum algorithm (following the seminal ideas of [1,2,3,4]) consists in three steps. First, encoding the data in a suitable initial quantum state. Second, driving such a state by a convenient sequence of unitary transformations until a final quantum state is reached (that can be implemented by quantum gates, resembling the microdesign of classical algorithms from logical states[5]). Third, measuring the final state and use such a measurement to solve the problem the quantum algorithm was designed for. For instance, in Grover[6] and Shor[7] algorithms (the most well-known quantum algorithms), the initial state is a uniform superposition of computational basis states. It encodes the elements of the unsorted database to look for, in the first case, and a representation of an approximation to the inverse of the period of an element in the residual group of units mod N, where N is the integer to factor, in the second case. The sequence of unitary transformations in those algorithms is an iterative composition of the oracle function (which encodes the elements of the data base to be found) and the diffusion operator (Grover's algorithm), or a sequence of controlled powers of a unitary operator (which encodes the modular multiplication by the element of the residual of units mod N) followed by an inverse quantum Fourier transform (Shor's algorithm). The measurement of the final state of Grover's algorithm provides (with probability approaching to one as the size of the database increases) a desired

element in the database, whereas the measurement of the final state of Shor's algorithm can be used to approximate the order on an invertible element mod N, which can be used to factor N (under certain circumstances).

An alternative description of quantum algorithms is provided by the stabilizer formalism[5]. In this paradigm, the focus is on the subgroup of elements of the Pauli group stabilizing the initial quantum state, and the transformations that such a subgroup experiments along the algorithm. Originally introduced in connection with quantum error correcting codes[8,9], it can be also used to provide alternative description and understanding of some quantum algorithms.

In this work, we provide an explanation of two classical quantum algorithms (Bernstein-Vazinari (BV)[10] and Deutsch-Josza (DJ)[4]) based on such a quantum stabilizer formalism. Doing so, we provide a better understanding and insight into both procedures which yield to see BV as a particular case of DJ, and to introduce a generalized version of DJ algorithm.

The outline of this paper is as follows. Preliminaries on the quantum stabilizer formalism are collected in Section 2. Section 3 is devoted to the explanation of the BV and DJ algorithms under the quantum stabilizer formalism. In Section 4, we consider a possible extension of these problems, based on the understanding provided by the stabilizer paradigm. Finally, conclusions and future directions of research can be found in Section 5.

2 | THE STABILIZER FORMALISM

In this preliminary section, we introduce notation, and collect well-known facts of quantum computing.

Computational quantum states

In this paper, $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$ will be a 2^n-dimensional Hilbert space of $n \geq 1$ qubits, with a computational basis $B = \{|i\rangle \ : \ i \in \mathbb{F}_2^n\}$ (here $\mathbb{F}_2$ denotes the Galois field of two elements $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$[11]). Elements in $(\mathbb{C}^2)^{\otimes n}$, written $|x\rangle$, are given by the $\mathbb{C}-$linear combinations of the elements in B, i.e., $|x\rangle = \sum_{i\in\mathbb{F}_2^n} \lambda_i |i\rangle$. The coefficients λ_i are called "amplitudes", and the element is assumed to be normalized, i.e., of complex norm equal to one: $\|x\| = \sqrt{\langle x|x\rangle}$ (here $\langle x|$ denotes the transpose conjugate of the element x, i.e., $\langle x| = \left(\sum_{i\in\mathbb{F}_2^n} \overline{\lambda_i}|i\rangle\right)^T$). Normalized quantum states are the states used in quantum computation.

Evolution of the quantum states

A complex $2^n \times 2^n-$invertible matrix $U = (U_{kl})_{1\leq k,l\leq n} \in GL(2^n, \mathbb{C})$ will be called "unitary" if $U \cdot U^\dagger = U^\dagger \cdot U = I_{2^n}$, where $U^\dagger = (\overline{U_{lk}})_{1\leq k,l\leq n}$ denotes its conjugate transposed matrix. These matrices represent the set of possible transformations that can be driven by a quantum computation, which has a group structure under multiplication, denoted $U(2^n)$ and called "unitary group". Another important class of matrices is given by the Hermitian ones, i.e., those $H \in U(2^n)$ such that $H = H^\dagger$. The set of Hermitian matrices is a $\frac{2^n(2^n+1)}{2}-$dimensional complex vector space, which is related to the unitary group via the Schrödinger equation $H(t)|x(t)\rangle = i\hbar\frac{d}{dt}|x(t)\rangle$, where $H(t)$ denotes the Hamiltonian driving the time-dependent quantum state $|x(t)\rangle$, i is the complex unity, and $\hbar$ is Planck reduced constant[5, 2.2.2]. Such a Hamiltonian is given by a Hermitian matrix, and the solution to such an equation is $U(t)|x(0)\rangle$, where $U(t) = e^{-i\frac{H(t)}{\hbar}}$ is a unitary matrix.

Measurements

Measures of a quantum state $|x\rangle$ are given by a set of "measurement operators" $\{M_m\}_{m\in\mu} \subseteq \mathcal{M}_{2^n}(\mathbb{C})$, where $\mu \in \mathbb{N}$, satisfying the "completeness equation" $I_{2^n} = \sum_{m\in\mu} M_m^\dagger M_m$. The output of such a measure on $|x\rangle$ is probabilistically the vector $M_m|x\rangle$, suitably normalized by the square of $p(m) = \langle x|M_m|x\rangle$ (i.e., $\langle x|M_m \cdot x\rangle$). The number $p(m)$ represents the actual probability of such a measure. Usually, measures are carried over the computational state basis, and so the measurement operators are $\{|i\rangle\langle i|\}_{i\in\mathbb{F}_2^n}$. In this case, the probability of obtaining $|i\rangle$ after measurement of the quantum state $\sum_{i\in\mathbb{F}_2^n} \lambda_i|i\rangle$ is $|\lambda_i|^2 = \overline{\lambda_i} \cdot \lambda_i$.

The Pauli group

A particular important set of $2 \times 2-$matrices, both unitary and Hermitian, are the Pauli matrices:

$$\left\{ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

The subgroup G_1 of $U(2)$ generated by such matrices has 16 elements, and can be written as

$$G_1 = \left\{ i^k X^a Z^b \mid 0 \leq k \leq 3, \ a, b \in \mathbb{F}_2 \right\}$$

Because $XZ = -iY$, the set $\{I_2\ ,\ X\ ,\ Z\ ,\ XZ\}$ is a $\mathbb{C}-$ basis of $\mathcal{M}_2(\mathbb{C})$. The $n-th$ tensor product of G_1 is known as the Pauli Group G_n, that can be written as

$$G_n = \left\{i^k X(a)Z(b) \mid 0 \leq k \leq 3\ ,\ a, b \in \mathbb{F}_2^n\right\} \leq U(2^n)$$

where $X(a) = X_1^{a_1} \otimes \cdots \otimes X_n^{a_n} = \bigotimes_{l=1}^n X_l^{a_l}$, and $Z(b) = Z_1^{b_1} \otimes \cdots \otimes Z_n^{b_n} = \bigotimes_{l=1}^n Z_l^{b_l}$. This subgroup has order 2^{2n+2}, and the subfamily $B = \{X(a)Z(b) \mid a, b \in \mathbb{F}_2^n\}$ of elements with trivial global phase (i.e, with $k = 0$), is a complex basis of the vector space $\mathcal{M}_{2^n}(\mathbb{C})$. Moreover, such a basis is orthonormal with respect to the Hermitian inner product $\langle A|B\rangle = \frac{1}{2^n}\mathrm{Tr}(A^\dagger \cdot B)$, for all $A, B \in \mathcal{M}_{2^n}(\mathbb{C})$ ($\mathrm{Tr} : \mathcal{M}_{2^n}(\mathbb{C}) \to \mathbb{C}$ denotes the trace function, i.e., the sum of elements on the main diagonal of matrix).

Centralizer of subgroups of the Pauli group

If for any $U = i^k X(a)Z(b) \in G_n$, we denote $w(U) = (a|b) \in \mathbb{F}_2^{2n}$, then the group commutator $[i^k X(a)Z(b)\ ,\ i^l X(c)Z(d)]$ is equal to $(-I_{2^n})^{(a|b)\star(c|d)}$, where $(a|b) \star (c|d) = a \cdot d + b \cdot c$ is a nondegenerate bilinear symplectic form on $\mathbb{F}_2^{2n}$ (here $\cdot$ denotes the standard inner product in $\mathbb{F}_2^n$). This means that:

- $\star$ is linear in both arguments: $(\lambda_1 a_1 + \lambda_2 a_2|\lambda_1 b_1 + \lambda_2 b_2)\star(c|d) = \lambda_1((a_1|b_1)\star(c|d)) + \lambda_2((a_2|b_2)\star(c|d))$, and $(a|b)\star(\lambda_1 c_1 + \lambda_2 c_2|\lambda_1 d_1 + \lambda_2 d_2) = \lambda_1((a|b)\star(c_1|d_1)) + \lambda_2((a|b)\star(c_2|d_2))$, for all $\lambda_1, \lambda_2 \in \mathbb{F}_2, a_1, a_2, a, b_1, b_2, b, c_1, c_2, c, d_1, d_2, d \in \mathbb{F}_2^n$)
- $(a|b) \star (a|b) = 0$, for all $a, b \in \mathbb{F}_2^n$
- For all nonzero $(a|b) \in \mathbb{F}_2^{2n}$, there exists $(c|d) \in \mathbb{F}_2^{2n}$ such that $(a|b) \star (c|d) \neq 0$

From here, it follows that if S is a nonempty subset of G_n, then its centralizer $C_{G_n}(S)$ is equal to $\{U \in G_n \mid w(U) \perp w(T)$, for all $T \in S\}$. It will be denoted by $S^\perp$. In particular, the center of G_n is $Z(G_n) = \{i^k I_{2^n} \mid 0 \leq k \leq 3\}$, a cyclic group of order 4, and $w : G_n/Z(G_n) \to \mathbb{F}_2^{2n}$ is a well-defined group isomorphism (from a multiplicative group to an additive group). The "quantum weight" of an element $U \in G_n$, is defined as the number of $1 \leq i \leq n$ such that $a_i \neq 0$ or $b_i \neq 0$, where $w(U) = (a|b)$.

2.1 | The main theorem of the stabilizer formalism

The following result is the fundamental basis of the stabilizer formalism.

Theorem 1. Let S be a subgroup of G_n. Then, the set $V_S = \{|x\rangle \mid U|x\rangle = |x\rangle\ ,\ \forall U \in S\}$ is nonzero if and only if $-I_{2^n} \notin S$. In such a case:

1. The map $w|_S : S \to \mathbb{F}_2^{2n}$ is a group monomorphism.
2. S is an elementary abelian $2-$subgroup of dimension $1 \leq n - k \leq n$ (i.e., S isomorphic to the additive group $\mathbb{F}_2^{n-k}$) and, correspondingly, $w(S)$ is a totally isotropic subspace of $(\mathbb{F}_2^{2n}\ ,\ \star)$ (i.e., $(a|b) \star (c|d) = 0$, for all $(a|b), (c|d) \in w(S)$).
3. $\mathbb{C}^{\otimes n}$ can be decomposed in 2^{n-k} eigenspaces of dimension 2^k, which can be indexed by the multiplicative characters of S according to the map
$$\begin{array}{ccc} \{\text{multiplicative characters of } S\} & \to & S = \{\text{eigenspaces of } \mathbb{C}^{2^n}\} \\ \chi & \to & J_\chi = \{|x\rangle \mid U|x\rangle = \chi(U)|x\rangle\ ,\ \forall U \in S\} \end{array}$$
so that V_S is indexed by the trivial character.
4. If $T \in U(2^n)$, then $(TST^\dagger)(T|x\rangle) = T|x\rangle$, for all $|x\rangle \in (\mathbb{C}^2)^{\otimes n}$. In particular, if C_n denotes the normalizer of G_n in $U(2^n)$ (i.e., the "Clifford group"), then $T|x\rangle \in V_{TST^\dagger}$, for all $|x\rangle \in V_S$ and $T \in C_n$.
5. More generally, G_n acts on the set $\mathcal{S}$ (via $T \cdot J_\chi = \{T|x\rangle \mid |x\rangle \in J_\chi\}$), so that the stabilizer subgroup of V_S (i.e., the elements T of G_n such that $T \cdot V_S = V_S$) is $S^\perp$, and S is the subgroup of G_n stabilizing V_S elementwise.

Proof. It can be found in [5, 10.5] and [12], but we stated it here for completeness. The condition $-I_{2^n} \notin S$ is clearly necessary (as such an operator does not fix any quantum state). Let us now assume that $-I_{2^n} \notin S$. We shall verify items 1 to 5 while proving that $V_S \neq 0$.

- Items 1 and 2: Since $-I_{2^n} \notin S$, then any nonidentity element in G_n has order 2. This is because $((i^k)X(a)Z(b))^4 = I_{n^2}$, and so the possible orders for nonidentity elements are 2 or 4. But, $((i^k)X(a)Z(b))^2 = i^{2k}I_{n^2}$, which is $-I_{n^2}$, unless $k = 0, 2$, i.e., unless the element has order 2. Now, S must be abelian, because all the elements in S are self-invertible (they are either the identity, or they have order 2), and so for all $U, T \in S$ we have

$$ST = ST \cdot ST \cdot TS = (ST)^2 \cdot (TS) = I_{n^2} \cdot (TS) = TS$$

Incidentally, this proves the first part of item 2, for some dimension $0 \leq n - k \leq n$. Moreover, because of the hypothesis, the restriction $w|_S$ is clearly a group monomorphism, since in S there can only exist at most one represent of each class of $G_n/Z(G_n)$ (namely, $Z(a)Z(b)$), and the map is straightforwardly an homomorphism. This proves item 1, and also gives us the second part of item 2, because of the relation between the commutator of two operators, and the corresponding bilinear form $\star$.

- Items 3, 4 and 5: Now, assuming that $S_1, \ldots, S_{n-k}$ is a $\mathbb{F}_2-$basis of S, we shall see item 3, by induction on $n - k$. As a consequence, we deduce $V_S \neq 0$.

  - The case $n - k = 1$ is straightforward, since S_1 has order 2, which forces its eigenvalues to be ± 1, and its trace to be zero. This makes 2^{n-1} eigenvalues equal to 1, and 2^{n-1} eigenvalues equal to -1, which is the base case of induction (there are two $2^{n-1}-$dimensional eigensubspaces, indexed by the trivial character and its opposite).
  - Now, assume that the case $n - k - 1$ is true, and let us prove the case $n - k$. By induction, $\langle S_1, \ldots, S_{n-k-1}\rangle$ decomposes $(C^2)^{\otimes n}$ in 2^{n-k-1} eigenspaces of dimension 2^{k+1}, indexed by the multiplicative characters of $\langle S_1, \ldots, S_{n-k-1}\rangle$, with $V_{\langle S_1,\ldots,S_{n-k-1}\rangle}$ indexed by the trivial character. Let J_η be one of such eigenspaces indexed by the character η of $\langle S_1, \ldots, S_{n-k-1}\rangle$. Let us prove that S_{n-k} leaves invariant J_η.
    Namely, for all $|x\rangle \in J_\eta$, and for all $U \in \langle S_1, \ldots, S_{n-k-1}\rangle$, since S_{n-k} commutes with $S_1, \ldots, S_{n-k-1}$, it commutes with $\langle S_1, \ldots, S_{n-k-1}\rangle$, and so

$$US_{n-k}|x\rangle = S_{n-k}U|x\rangle = S_{n-k}\eta(U)|x\rangle = \eta(U)S_{n-k}|x\rangle$$

    Observe that $\eta(U) \in \mathbb{C}$, because S in an abelian group. This means that $S_{n-k}|_{J_\eta} : J_\eta \to J_\eta$ is an isomorphism of vector spaces.
    Now, since $w|_S : S \to \mathbb{F}_2^{2n}$ is a monomorphism, and $\star$ is nondegenerate, there exists $T \in G_n$ such that $w(T) \star w(S_i) = \delta_{i,n-k}$, i.e., such that T anticommutes with S_{n-k}, and commutes with the other S_i. Therefore, for all $|x\rangle \in J_\eta$, we have

$$S_iT|x\rangle = (TS_iT^\dagger)T|x\rangle = TS_i|x\rangle = T\eta(S_i)|x\rangle = \eta(S_i)T|x\rangle$$

    for all $1 \leq i \leq n - k - 1$, i.e., $T|x\rangle \in J_\eta$, observe that the same technique can be used to prove items 4 and 5.
    Now, if $|x\rangle \in J_\eta$ is an eigenvector of S_{n-k} with eigenvalue λ, then

$$S_{n-k}T|x\rangle = (-TS_{n-k}T^\dagger)T|x\rangle = -TS_{n-k}|x\rangle = -T\lambda|x\rangle = -\lambda T|x\rangle$$

    that is, $T|x\rangle \in J_\eta$ is an eigenvector of S_{n-k} with eigenvalue $-\lambda$. So, the eigenvalues of $S_{n-k}|_{J_\eta}$ come in pairs $\{1, -1\}$ (one corresponding to an eigenvector $|x\rangle$, the other one corresponding to the eigenvector $T|x\rangle$), and so each J_η is decomposed as two eigenspaces of dimension 2^k: J_η^+, and J_η^-.
    The set of 2^{n-k} eigenspaces of dimension 2^k, is indexed by the multiplicative characters of $\langle S_1, \ldots, S_{n-k}\rangle$, namely $J_\chi = J^{\chi(S_{n-k})}_{\chi_{\langle S_1,\ldots,S_{n-k-1}\rangle}}$ (i.e., the multiplicative character χ is equal to η, when restricted to $\langle S_1, \ldots, S_{n-k-1}\rangle$, and it is $\chi(S_{n-k}) = \pm 1$). The trivial character clearly indexes $V_{\langle S_1,\ldots,S_{n-k}\rangle}$, which is so nonzero.

□

This theorem states that, up to a global phase, there is a correspondence between certain quantum states of $(\mathbb{C}^2)^{\otimes n}$ and elementary abelian $2-$subgroups of G_n of dimension n. Moreover, any quantum computation carried out by operators of the Clifford group on one of those states is directly translated into a conjugation operation in the Pauli group. So, certain quantum algorithms that involve circuits containing quantum gates from the Clifford group can be classically simulated (efficiently) by tracking conjugates of n elements of the Clifford group. This fact, along with the corresponding efficiency in the measures described in[5, 10.5.3], is known as the "Gottesman-Knil theorem"[13].

Example

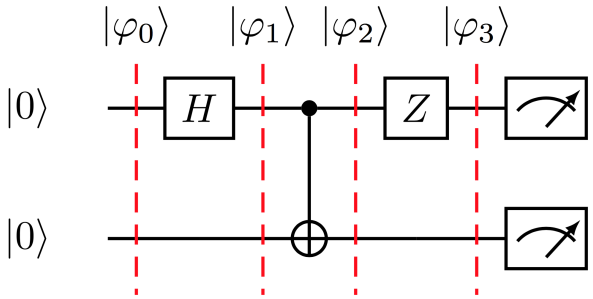

FIGURE 1 Example quantum circuit

Let us illustrate the stabilizer paradigm with the circuit of Figure 1.

The initial state is $|\varphi_0\rangle = |0\rangle \otimes |0\rangle$, with stabilizer subgroup S_0 generated by $Z_1 = I \otimes Z$, and $Z_2 = Z \otimes I$. Application of the Hadamard gate in the first qubit transforms $|\varphi_0\rangle$ into $|\varphi_1\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle$. The corresponding subgroup is obtained by conjugation of $\langle Z_1, Z_2\rangle$ by the element $H \otimes I$, i.e., it is $S_1 = \langle X_1 = X \otimes I, Z_2\rangle$. The control NOT gate yields the (Bell) state $|\varphi_2\rangle = \frac{|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle}{\sqrt{2}}$, and the corresponding stabilizer subgroup $S_2 = \langle X_1 \otimes X_2, Z_1 \otimes Z_2\rangle$. Right before the measurement, we have the quantum state $|\varphi_3\rangle = \frac{|0\rangle\otimes|0\rangle-|1\rangle\otimes|1\rangle}{\sqrt{2}}$ (another Bell state), whose stabilizer group is $S_3 = \langle -X_1 \otimes X_2, Z_1 \otimes Z_2\rangle$. Table 1 contains a summary of the quantum states and the stabilizer subgroups corresponding to the circuit of Figure 1.

Stage	Quantum state	Stabilizer subgroup
0	$\|0\rangle \otimes \|0\rangle$	$\langle Z_1, Z_2\rangle$
1	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}} \otimes \|0\rangle$	$\langle X_1, Z_2\rangle$
2	$\frac{\|0\rangle\otimes\|0\rangle+\|1\rangle\otimes\|1\rangle}{\sqrt{2}}$	$\langle X_1 \otimes X_2, Z_1 \otimes Z_2\rangle$
3	$\frac{\|0\rangle\otimes\|0\rangle-\|1\rangle\otimes\|1\rangle}{\sqrt{2}}$	$\langle -X_1 \otimes X_2, Z_1 \otimes Z_2\rangle$

TABLE 1 Quantum states and stablizer subgroups in the example

This formalism explains straighforwardly the familiy of quantum error correcting codes known as "stabilizer codes"[5, 10.5.5]. In this context, certain 2^k-dimensional quantum error correcting codes V_S are described by the corresponding elementary abelian $2-$subgroups S of G_n of dimension $n-k$, known as "error group". The errors with no effect on the quantum state are those effected by elements of S, where as the undetectable errors are those in $S^\perp \setminus S$, since they transform the quantum state in another one belonging to the code. The correctable errors are subsets E of G_n such that whenever $T, U \in E$, then $T^{-1}U \notin S^\perp \setminus S$. This set is usually taken as those elements of the Pauli group of quantum weight not greater than $\lceil \frac{d-1}{2} \rceil$, where d is minimum quantum weight of the elements in $S^\perp \setminus S$[12].

3 | BV AND DJ ALGORITHMS

In this section we explain BV and DJ algorithms with the stabilizer formalism introduced above. Both algorithms have quantum access to a binary function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ by an oracle $O : (\mathbb{C}^2)^{\otimes(n+1)} \to (\mathbb{C}^2)^{\otimes(n+1)}$, in the standard way $O(|x\rangle|y\rangle) = |x\rangle|x \oplus f(y)\rangle$, where $|x\rangle \in (\mathbb{C}^2)^{\otimes n}$, and $|y\rangle \in \mathbb{C}^2$. As usual, this oracle is managed in its phase oracle version, i.e., since $O(|x\rangle|-\rangle) = (-1)^{f(x)}|x\rangle|-\rangle$, for the single qubit element $|-\rangle = \frac{|0\rangle-|1\rangle}{2}$, the auxiliary last qubit is dropped and the corresponding oracle is $O_f|x\rangle = (-1)^{f(x)}|x\rangle$, for all $|x\rangle \in (\mathbb{C}^2)^{\otimes n}$.

3.1 | BV

The goal of the BV algorithm is to determine a linear function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ from its evaluations. That is, a certain function f is given under the promise that $f(x) = x \cdot s$, for some binary unknown array $s \in \mathbb{F}_2^n$ (here again $\cdot$ denotes the standard inner product in $\mathbb{F}_2^n$). Clasically, this problem requires $O(n)$ evaluations of f (that yield the solution of the corresponding linear system of equations). However, BZ only uses a single (quantum query) evaluation of f. The algorithm, whose quantum circuit can be found in Figure 2, is as follows.

BV algorithm

INPUT: A linear function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, with $f(x) = x \cdot s$, for all $x \in \mathbb{F}_2^n$
OUTPUT: A vector s
Set the initial quantum state $|0^{\otimes n}\rangle$
Apply the Walsh-Hadamard transform[5, 1.4.2] $H^{\otimes n}$, where $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the Hadamard gate
Apply the phase oracle O_f
Apply the Walsh-Hadamard transform $H^{\otimes n}$
If the measurement of the final state in the computational basis is $|s\rangle$, RETURN "s"

It can be proved that, with probability one, the final measurent gives the quantum state $|s\rangle$, for the desired unknown value s. Let us prove this fact under the stabilizer formalism, in a straightforward way.

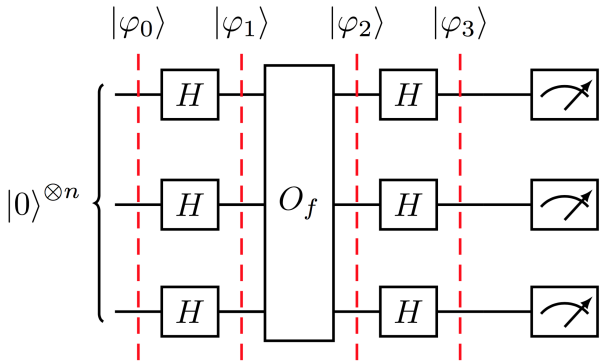

FIGURE 2 Quantum circuit of the BV algorithm

Since $|0\rangle$ is an eigenvector of the Pauli matrix Z (with eigenvalue 1), it is clear that the initial sate $|0^{\otimes n}\rangle$ is stabilized by any matrix of the form $Z(e_i)$, where $e_i = (0 \dots 0 \overset{(i}{1} 0 \dots 0)$ is an element in the standard basis of $\mathbb{F}_2^n$. The subgroup S of G_n generated by those n matrices is abelian, since the elements $\{e_i\}_{i=1}^n$ are pairwise orthogonal, with respect to the bilinear form $\star$ (i.e., $\mathbb{F}_2^n \times \{0\}$ is a totally isotropic subspace of $(\mathbb{F}_2^{2n}, \star)$).

Since $HZH^\dagger = X$, we have that application of the Walsh-Hadamard transform $H^{\otimes n}$ on the initial state, is equivalent to applying the conjugation by $H^{\otimes n}$ on each of the matrices $Z(e_i)$, and so the stabilizer subgroup is generated by the n matrices $\{X(e_i)\}_{i=1}^n$.

Now, it follows the application of the phase oracle O_f. Observe that, for all $1 \leq i \leq n$, and $s_i \in \mathbb{F}_2$, the operator $Z_i^{s_i}$ transforms the quantum state $|x\rangle$ of the computational basis, into $(-1)^{s_i \cdot x_i}|x\rangle$ (when $x_i = 0$, the state remains the same, and it takes an opposite global phase when $x_i = 1$). Therefore, because of linearity $O_f|x\rangle = (-1)^{f(x)}|x\rangle = (-1)^{x \cdot s}|x\rangle = (-1)^{x_1 \cdot s_1} \cdot \dots \cdot (-1)^{x_n \cdot s_n}|x\rangle = Z(s)|x\rangle$, for all $|x\rangle \in \mathbb{C}^{\otimes n}$. Hence, the action of the phase oracle on the quantum state is translated into conjugation by the element $Z(s)$, i.e., since $ZXZ^\dagger = -X$, those $1 \leq i \leq n$ with $s_i = 0$ have an unmodified $X(e_i)$ as generator of the stabilizer subgroup, whereas those with $s_i = 1$ provide by conjugation the generator $-X(e_i)$. Summarizing, the stabilizer

subgroup is generated by $\{(-1)^{s_i}X(e_i)\}_{i=1}^n$. Incidentally, notice that the oracle O_f, is an element of the Pauli group (and so in particular of the Clifford group), so the algorithm can be efficiently realised via the Gottesman-Knill theorem.

A second application of the operator $H^{\otimes n}$, because of the relation $HXH^\dagger = Z$, yields that the stabilizer subgroup finally achieved is generated by the n matrices $\{(-1)^{s_i}Z(e_i)\}_{i=1}^n$.

Since the Z matrix stabilizes the qubit $|0\rangle$, and $-Z$ stabilizes the qubit $|1\rangle$, we have that, for all $1 \leq i \leq n$, and $a \in \mathbb{F}_2$, the matrix $(-1)^a Z$ stabilizes the quantum state $|a\rangle$. Therefore, the state stabilized by the last subgroup is exactly $|s\rangle$, and so the final measure of the algorithm gives $|s\rangle$ with probability one. A summary of the quantum states and the stabilizer subgroups corresponding to BV algorithm, can be found in Table 2.

Stage	Quantum state	Stabilizer subgroup
0	$\|0^{\otimes n}\rangle$	$\langle Z_1, \dots, Z_n\rangle$
1	$\frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{F}_2^n}\|x\rangle$	$\langle X_1, \dots, X_n\rangle$
2	$\frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{F}_2^n}(-1)^{s\cdot x}\|x\rangle$	$\langle (-1)^{s_1}X_1, \dots, (-1)^{s_n}X_n\rangle$
3	$\|s\rangle$	$\langle (-1)^{s_1}Z_1, \dots, (-1)^{s_n}Z_n\rangle$

TABLE 2 Quantum states and stablizer subgroups in the BV algorithm

3.2 | DJ

The goal of the DJ algorithm is to determine if a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is constant or balanced. That is, a certain function f is given under the promise that it is constant (i.e., $f = 0$ or $f = 1$) or balanced (i.e., $M = \#\{x \in \mathbb{F}_2^n \mid f(x) = 1\} = 2^{n-1}$. Clasically, this problem requires $O(2^{n-1})$ evaluations of f (half plus one evaluations are needed in the worst case to distinguish a constant or balanced function). However, DJ only uses a single (quantum query) evaluation of f. The algorithm, whose quantum circuit can be found in Figure 3, is as follows. Observe that, except for the decision taken after the final measurement, the steps of the BV and DJ algorithms are the same. This explains why Figure 2 and 3 are the same.

Deutsch-Josza algorithm

INPUT: A boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, promised to be either constant or balanced
OUTPUT: "f CONSTANT" or "f BALANCED"
Set the initial quantum state $|0^{\otimes n}\rangle$
Apply the Walsh-Hadamard transform $H^{\otimes n}$, where $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the Hadamard gate
Apply the phase oracle O_f
Apply the Walsh-Hadamard transform $H^{\otimes n}$
If the measurement of the final state in the computational basis is $|0^{\otimes n}\rangle$, RETURN "f CONSTANT".
Else, RETURN "f BALANCED"

It can be proved that, with probability one, the final measurement gives the quantum state $|0^{\otimes n}\rangle$ if and only if f is constant. When f is balanced, it gives other element of the computational basis. The first two steps in DJ are those of BV, and so the stabilizer subgroup is generated by the n matrices $\{X(e_i)\}_{i=1}^n$ after them.

Observe that the quantum circuit of DJ is just like that of BV.

Now, it follows the application of the phase oracle O_f. An alternative formulation of this operator is the following one: $O_f = I_{2^n} - 2\sum_{x\in M}|x\rangle\langle x|$, because $O_f|x\rangle = |x\rangle$ if and only if $x \notin M$ (i.e., iff $f(x) = 0$), and $O_f|x\rangle = -|x\rangle$, when $x \in M$. Because $B = \{X(a)Z(b) \mid a, b \in \mathbb{F}_2^n\}$ is is an orthonormal basis of $\mathcal{M}_{2^n}(\mathbb{C})$ with respect to $\langle A|B\rangle = \frac{1}{2^n}\mathrm{Tr}(A^\dagger \cdot B)$, it is straightforward to write O_f as a linear combination of the elements in B (the coefficients are given by $\langle O_f|X(a)Z(b)\rangle$, for all $a, b \in \mathbb{F}_2^n$). When f is constant, then $O_f = \pm I_{n^2}$, and so $O_f = \pm X(0^n)Z(0^n)$, where 0^n is the zero vector of $\mathbb{F}_2^n$. When f is

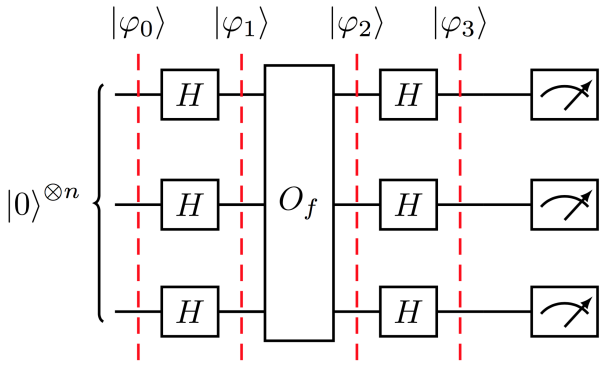

FIGURE 3 Quantum circuit of the DJ algorithm

balanced, notice first that, for all $a \in \mathbb{F}_2$, $X|a\rangle = |\overline{a}\rangle$ (here $\overline{a}$ is the complement of a mod 2), that $I_{2^n}|a\rangle = \pm Z|a\rangle = |a\rangle$. Also, observe that $\mathrm{Tr}(X) = \mathrm{Tr}(XZ) = 0$, so consequently $\mathrm{Tr}(X(a)Z(b)) = 0$ if $a \neq 0^n$. Hence, for all $a, b \in \mathbb{F}_2^n$,

$$2^n \cdot \langle O_f|X(a)Z(b)\rangle = \mathrm{Tr}(O_f^\dagger \cdot X(a)Z(b)) = \mathrm{Tr}\left(\left(I_{n^2} - 2\sum_{x\in M}|x\rangle\langle x|\right)\cdot X(a)Z(b)\right)$$

$$= \mathrm{Tr}\left(X(a)Z(b) - 2\left(\sum_{x\in M}|x\rangle\langle x|X(a)Z(b)\right)\right)$$

$$= \mathrm{Tr}(X(a)Z(b)) - 2\sum_{x\in M}\mathrm{Tr}\left(|x\rangle\langle x|X(a)Z(b)\right) = \mathrm{Tr}(X(a)Z(b)) - 2\sum_{x\in M}\langle x|X(a)Z(b)|x\rangle$$

and we have two particular cases:

- $a = b = 0^n$, where $2^n \cdot \langle O_f|X(0^n)Z(0^n)\rangle = \mathrm{Tr}(I_{n^2}) - 2\sum_{x\in M}\langle x|x\rangle = 2^n - 2\cdot\sum_{x\in M}1 = 0$
- $a \neq 0^n$, where $2^n \cdot \langle O_f|X(a)Z(b)\rangle = \mathrm{Tr}(X(a)Z(b)) - 2\sum_{x\in M}\langle x|X(a)Z(b)|x\rangle = 0 - 2\cdot\sum_{x\in M}0 = 0$

Hence, O_f can be expressed as a nontrivial complex linear combination of the elements in the set $\{Z(b) \mid b \in \mathbb{F}_2^n \setminus \{0^n\}\}$. Remember, from the analysis of BV, that the elements in this set correspond to phase oracles of nonzero linear functions. However, unlike BV, this oracle might not correspond to an element of the Clifford group (and as a consequence the algorithm might not be efficiently realisable via the Gottesman-Knill theorem). A measurement of the realizability of the algorithm is the "stabilizer rank"[14], which in this case is upper bounded by the number of nonzero coefficients of O_f as a linear combination of the elements in the set $\{Z(b) \mid b \in \mathbb{F}_2^n \setminus \{0^n\}\}$.

Coming back to the stabilizer formalism analysis of DJ, we have that $O_f = \pm I_{n^2}$, when f is constant, and that $O_f = \sum_{b\in\mathbb{F}_2^n}\lambda_b Z(b)$, for certain complex numbers $\lambda_b = \langle O_f|Z(b)\rangle$ (with $\lambda_{0^n} = 0$), when f is balanced. Hence, the action of the phase oracle on the third step of DJ, is translated into conjugation by either $\pm I_{n^2}$, or by a nontrivial linear combination of operators $Z(b)$, with $b \neq 0$. In the first case, the stabilizer group after this step is again the one generated by $\{X(e_i)\}_{i=1}^n$. In the second case, since $Z(b)X(e_i)Z(b')^\dagger = (-1)^{b_i}X(e_i)Z(b\oplus b')$, the stabilizer subgroup is $O_f\langle X(e_1),\ldots,X(e_n)\rangle O_f^\dagger = \left\langle X(e_i)\left(\sum_{b,b'\in\mathbb{F}_2^n}\lambda_b\overline{\lambda_{b'}}(-1)^{b_i}Z(b\oplus b')\right)\right\rangle_{i=1}^n$ (where $\oplus$ denotes addition in $\mathbb{F}_2^n$).

The second application of the operator $H^{\otimes n}$, yields in the first case a stabilizer subgroup generated by the n matrices $\{Z(e_i)\}_{i=1}^n$, and the corresponding stabilized state is $|0^{\otimes n}\rangle$, which is to be measured with probability one. In the second case, the n elements generating the stabilizer subgroup are $H^{\otimes n}O_f\langle X(e_1),\ldots,X(e_n)\rangle O_f^\dagger H^{\otimes n} = \left\langle Z(e_i)\left(\sum_{b,b'\in\mathbb{F}_2^n}\lambda_b\overline{\lambda_{b'}}(-1)^{b_i}X(b\oplus b')\right)\right\rangle_{i=1}^n$. This subgroup stabilizes the quantum state $\sum_{b\in\mathbb{F}_2^n}\lambda_b|b\rangle$, because

$$H^{\otimes n}\left(\sum_{b\in\mathbb{F}_2^n}\lambda_b|b\rangle\right) = \sum_{b\in\mathbb{F}_2^n}\lambda_b H^{\otimes n}|b\rangle = \sum_{b\in\mathbb{F}_2^n}\lambda_b\sum_{x\in\mathbb{F}_2^n}\frac{(-1)^{x\cdot b}}{\sqrt{2^n}}|x\rangle = \sum_{b\in\mathbb{F}_2^n}\lambda_b\sum_{x\in\mathbb{F}_2^n}\frac{Z(b)}{\sqrt{2^n}}|x\rangle$$

$$= \left(\sum_{b \in \mathbb{F}_2^n} \lambda_b Z(b) \right) \left(\sum_{x \in \mathbb{F}_2^n} \frac{|x\rangle}{\sqrt{2^n}} \right) = O_f H^{\otimes n} |0^{\otimes n}\rangle$$

and so $H^{\otimes n} O_f H^{\otimes n} |0^{\otimes n}\rangle = \sum_{b \in \mathbb{F}_2^n} \lambda_b |b\rangle$. The result is derived from Theorem 1 (item 4).

Finally, since $\lambda_0 = 0$, the measurement yields with probability one $|0^{\otimes n}\rangle$ if and only if f is constant. A summary of the quantum states and the stabilizer subgroups corresponding to DJ algorithm, can be found in Table 3.

Stage	Quantum state		Stabilizer subgroup	
	f constant	f balanced	f constant	f balanced
0	$\|0^{\otimes n}\rangle$		$\langle Z_1, \dots, Z_n \rangle$	
1	$\frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_2^n} \|x\rangle$		$\langle X_1, \dots, X_n \rangle$	
2	$\pm \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_2^n} \|x\rangle$	$\pm \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} \|x\rangle$	$\langle X_1, \dots, X_n \rangle$	$O_f \langle X_1, \dots, X_n \rangle O_f^\dagger$
3	$\pm \|0^{\otimes n}\rangle$	$\sum_{b \in \mathbb{F}_2^n} \lambda_b \|b\rangle$	$\langle Z_1, \dots, Z_n \rangle$	$H^{\otimes n} O_f \langle X_1, \dots, X_n \rangle O_f^\dagger H^{\otimes n}$

TABLE 3 Quantum states and stablizer subgroups in the DJ algorithm

4 | BEYOND THE KNOWN ALGORITHMS: GENERALIZED DJ

In this section, we consider a possible extension of the BV and DJ algorithms, based on the understanding provided by the stabilizer paradigm of the previous section. First, we remark is that the BV algorithm can be seen (except by its output), as a particular case of the DJ algorithm. Namely, in both algorithms, all the steps except for the last one are exactly the same. Moreover, being linear any promised function for the BV algorithm, such a function must be either $f = 0$ or balanced (the set $\mathbb{F}_2^n \setminus \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ is the kernel of the $\mathbb{F}_2-$linear function f, and so its cardinality is $\frac{2^n}{2}$, because its image is $\mathbb{F}_2$). Therefore, when measured with probability one, the output state $|0^{\otimes n}\rangle$ occurs if and only if f is constant (i.e., $f = 0$). In any other case, the function is balanced. Moreover, in the case $n = 1$, the two balanced functions are the only nonzero linear ones (with oracle $O_f = Z(1)$), and its complementary function (with oracle $O_f = -Z(1)$). So, BV is exactly the same as DJ (which in this case is called "Deutsch Algorithm"[15]).

Secondly, we want to remark on the nature of the DJ oracle, that is expressed as $\sum_{b \in \mathbb{F}_2^n} \lambda_b Z(b)$. This expression is not exclusive of the oracle of balanced or constant functions, but of any arbitrary boolean function, too. If we consider the analysis of the DJ algorithm, the condition "f balanced" is only used to deduce that $\lambda_{0^n} = 0$, so such an expression is valid for any function $f : \mathbb{F}_2^n \to \mathbb{F}_2$. So, if we apply any of the two algorithms to an arbitrary boolean function f, the final measurement would be $|b\rangle$, one of the states of the computational basis that appears in the description of the corresponding oracle O_f. The probability of such a measurement is exactly $\left| \frac{1}{2^n} \mathrm{Tr}(O_f^\dagger \cdot Z(b)) \right|^2$.

Finally, from the point of view of the connections with quantum error correcting codes and the stabilizer formalism, we can "see" BV and DJ as the decoding procedure of errors introduced by the "perturbations" $Z(b)$ involved in the linear combination of the oracle O_f. The measurement $|s\rangle$ is, therefore, one of the possible syndromes induced by such perturbations. This lead us to introduced a generalization of the DJ problem, for each possible syndrome $s \in \mathbb{F}_2^n$.

Generalized DJ problem:

Given a vector $s \in \mathbb{F}_2^n$, and a boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, with the promise that the function $f \oplus s$ is either constant or balanced, determine which is the case.

A solution of this problem is given by the:

Generalized DJ algorithm:

INPUT: A vector $s \in \mathbb{F}_2^n$, and a boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, with the promise that the function $g = f \oplus s$ is either constant or balanced

OUTPUT: "g CONSTANT" or "g BALANCED"

Set the initial quantum state $|0^{\otimes n}\rangle$

Apply the Walsh-Hadamard transform $H^{\otimes n}$, where $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the Hadamard gate

Apply the phase oracle O_f

Apply the Walsh-Hadamard transform $H^{\otimes n}$

If the measurement of the final state in the computational basis is $|s\rangle$, RETURN "g CONSTANT".

Else, RETURN "g BALANCED"

This algorithm gives the right answer to the Generalized DJ problem, with probability one. The reason is that, since for all $x \in \mathbb{F}_2^n$, we have $O_g|x\rangle = (-1)^{g(x)}|x\rangle = (-1)^{s\cdot x}(-1)^{f(x)}|x\rangle = (-1)^{s\cdot x}O_f|x\rangle = O_f(-1)^{s\cdot x}|x\rangle = O_f Z(s)|x\rangle$. Therefore, the algorithm returns "g BALANCED" if and only if the final measurement is not $|s\rangle$, if and only if $\frac{1}{2^n}\mathrm{Tr}(O_f^\dagger \cdot Z(s))$ is zero, if and only if $\mathrm{Tr}(O_g^\dagger) = 0$, if and only if g is really balanced (because $g = \sum_{0\neq b\in\mathbb{F}_2^n} \mu_b Z(b)$, with $\mu_b = \mathrm{Tr}(O_g^\dagger \cdot Z(b))$, since $\mu_{0^n} = 0$).

5 | CONCLUSIONS AND FUTURE WORK

In this paper, we have presented an explanation of the correctness of the BV and DJ algorithms based on the stabilizer formalism. This paradigm was initially introduced in connection to quantum error correcting codes, but it is useful to provide a better understanding of other techniques in quantum computation, like the ones considered here. Inspired by this link, we have introduced a generalised version of the DJ problem, and the corresponding algorithm that solves it. In the process, we have seen that the phase oracle of any boolean function can be expressed as a linear combination of tensor products of Z gates. And that the probability of measurement of a certain element in the computational basis, by the algorithms under study, is directly related to the coefficients of such a linear combination. Further inspired by this facts, we intend to explore a familiy of problems, that we call "quantum exact promise problems", in which a certain subset of boolean functions is partitioned into a collection of subsets which have to be distinguished from each other.

ACKNOWLEDGEMENTS

This work was supported in part by the MINECO under Grant MTM-2017-83506-C2-2-P and Grant MINECO-16-TEC2015-67387-C4-3-R, and in part by the MICINN under Grant RTI2018-098085-B-C44, Grant FC-GRUPIN-IDI/2018/000193, and under Grant FC-GRUPIN-IDI/2018/000226.

References

1. Feynman R. Simulating physics with computers. *International Journal of Theoretical Physics* 1982; 21 (6): 467-488.

2. Manin Y. Vychislimoe i nevychislimoe. *Sov. Radio* 1980: 13-15.

3. Benioff P. The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of statistical physics* 1980; 22 (5): 563-591.

4. Deutsch D, Jozsa R. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 1992; 439(1907): 553–558.

5. Nielsen MA, Chuang IL. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press . 2011.

6. Grover LK. A Fast Quantum Mechanical Algorithm for Database Search. In: STOC '96. ACM; 1996; New York, NY, USA: 212–219.

7. Shor PW. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In: SFCS '94. IEEE Computer Society; 1994; Washington, DC, USA: 124–134

8. Calderbank AR, Rains EM, Shor PW, Sloane NJA. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory* 1998; 44(4): 1369–1387. doi: 10.1109/18.681315

9. Gottesman D. Stabilizer codes and quantum error correction (Caltech Ph.D. thesis). https://arxiv.org/abs/quant-ph/9705052; 1997.

10. Bernstein E, Vazirani U. Quantum complexity theory. *SIAM J. Comput.* 1997; 26(5): 1411–1473. doi: 10.1137/S0097539796300921

11. Lidl R, Niederreiter H. *Finite Fields*. Encyclopedia of Mathematics and its Applications (20)Addison-Wesley . 1983.

12. Cameron PJ. Finite geometry and coding theory. https://cameroncounts.files.wordpress.com/2015/04/fgct.pdf; .

13. Gottesman D. The Heisenberg Representation of Quantum Computers. https://arxiv.org/abs/quant-ph/9807006v1; 1998.

14. Bravyi S, Browne D, Calpin P, Campbell E, Gosset D, Howard M. Simulation of quantum circuits by low-rank stabilizer decompositions. *Quantum* 2019; 3: 181.

15. Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. Roy. Soc. London Ser. A* 1985; 400(1818): 97–117.