Final Honour School of Mathematics Part C

C7.4 Introduction to Quantum Information
Artur Ekert
Checked by: Lionel Mason

March 2017

ABD: EveryShipout initializing macros

Do not turn this page until you are told that you may do so

1. (a) [2 marks] Describe the Hadamard gate and the controlled-NOT gate.

   (b) [3 marks] Draw a quantum network (circuit) that encodes a single qubit state $\alpha|0\rangle+\beta|1\rangle$ into the state $\alpha|00\rangle+\beta|11\rangle$ of two qubits. Here and in the following α and β are some unknown generic complex coefficients.

   (c) [5 marks] Two qubits were prepared in state $\alpha|00\rangle+\beta|11\rangle$, exposed to bit flip-errors, and then measured with an ancillary qubit, as shown in Fig. 1. The result of the measurement is x. Can you infer the absence of errors when $x=0$? Can you infer the presence of errors when $x=1$? Can you correct any detected errors?

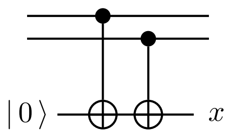


Fig. 1

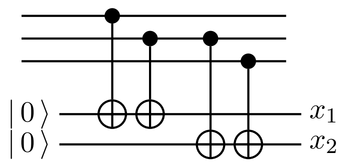


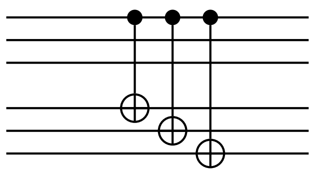
Fig. 2

Three qubits were prepared in state $\alpha|000\rangle+\beta|111\rangle$ and then, by mistake, someone applied the Hadamard gate to one of them, but nobody remembers which one. Your task is to recover the original state of the three qubits.

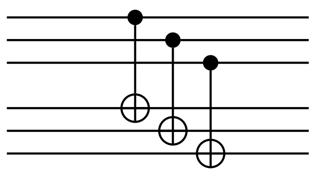
   (d) [4 marks] Express the Hadamard gate as the sum of two Pauli matrices. Pick up one of the three qubits and apply the Hadamard gate. How is the state $\alpha|000\rangle+\beta|111\rangle$ modified? Interpret this in terms of bit-flip and phase-flip errors.

   (e) [6 marks] You perform the error syndrome measurement shown in Fig. 2. Suppose the outcome of the measurement is $x_1=0, x_2=1$. How would you recover the original state? Describe the recovery procedure when $x_1=0, x_2=0$.

The figure below shows two implementations of a controlled-NOT gate acting on the encoded states of the three qubit code.



Implementation A



Implementation B

   (f) [5 marks] Assume that the only sources of errors are individual controlled-NOT gates which produce bit-flip errors in their outputs. These errors are independent and occur with a small probability p. For each of the two implementations find the probability of generating unrecoverable errors at the output. Which of the two implementations is fault-tolerant?

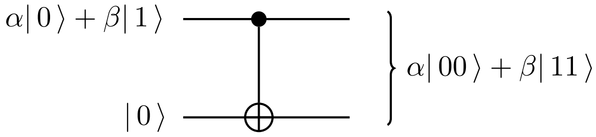
SOLUTION TO QUESTION 1.

(a) [2 marks] [Standard material] The Hadamard gate is a single qubit quantum gate that effects the unitary operation

$$\begin{aligned} |\,0\,\rangle &\mapsto \frac{1}{\sqrt{2}}\left(|\,0\,\rangle + |\,1\,\rangle\right), \\ |\,1\,\rangle &\mapsto \frac{1}{\sqrt{2}}\left(|\,0\,\rangle - |\,1\,\rangle\right). \qquad \text{[1 mark]} \end{aligned}$$

The controlled-NOT gate is a two-qubit quantum gate defined, in the computational basis, as: $|\,x\,\rangle|\,y\,\rangle \mapsto |\,x\,\rangle|\,y \oplus x\,\rangle$, where $x, y = 0, 1$. The bit value x of first qubit, called the controlled qubit, does not change, but the bit value y of the second qubit, called the target, is negated if $x = 1$ and retains its input value otherwise. The two gates are among the most popular quantum gates. [1 mark]

(b) [3 marks] [Standard bookwork] The controlled-NOT gate alone, with the target prepared in state $|\,0\,\rangle$, implements the required encoding.



(c) [5 marks] [New-ish but very similar to the three qubit code, which is standard material] Given the bit-flip errors, there are four possible scenarios: no errors, error on the first qubit, error on the second qubit and two errors. The action of the network in each of these four cases is :

$$\begin{aligned} (\alpha|\,00\,\rangle + \beta|\,11\,\rangle)|\,0\,\rangle &\mapsto (\alpha|\,00\,\rangle + \beta|\,11\,\rangle)|\,0\,\rangle \quad \text{no erros} \\ (\alpha|\,10\,\rangle + \beta|\,01\,\rangle)|\,0\,\rangle &\mapsto (\alpha|\,10\,\rangle + \beta|\,01\,\rangle)|\,1\,\rangle \quad \text{error on 1st qubit} \\ (\alpha|\,01\,\rangle + \beta|\,10\,\rangle)|\,0\,\rangle &\mapsto (\alpha|\,01\,\rangle + \beta|\,10\,\rangle)|\,1\,\rangle \quad \text{error on 2st qubit} \\ (\alpha|\,11\,\rangle + \beta|\,00\,\rangle)|\,0\,\rangle &\mapsto (\alpha|\,11\,\rangle + \beta|\,00\,\rangle)|\,0\,\rangle \quad \text{two errors} \qquad \text{[3 marks]} \end{aligned}$$

which shows that outcome $x = 0$ is inconclusive for it occurs both in the absence of errors and when there are two errors (one on each qubit). [1 mark]
The outcome $x = 1$ indicates one error, be it on the first or on the second qubit, which makes it impossible to correct it. The two qubit code is an error detection but not an error correction code. [1 mark]

(d) [4 marks] [New] The Hadamard gate can be written as $H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$ thus acting on the code state $\alpha|\,000\,\rangle + \beta|\,111\,\rangle$ it will create a superposition of two terms corresponding to the code state with the phase-flip error σ_z and the code state with a bit-flip error σ_x. For example, if the Hadamard was applied to the third qubit we obtain

$$\begin{aligned} \alpha|\,000\,\rangle + \beta|\,111\,\rangle &\mapsto \frac{1}{\sqrt{2}}\left[\alpha|\,00\,\rangle(|\,0\,\rangle + |\,1\,\rangle) + \beta|\,11\,\rangle(|\,0\,\rangle - |\,1\,\rangle)\right] \\ &= \frac{1}{\sqrt{2}}\left[(\alpha|\,000\,\rangle - \beta|\,111\,\rangle) + (\alpha|\,001\,\rangle + \beta|\,110\,\rangle)\right] \qquad \text{[2 marks]} \end{aligned}$$

The first term corresponds to the phase-flip error which can be attributed to any of the three qubits (even though it originates from the qubit to which the Hadamard gate was applied). The second term corresponds to the bit-flip error on the qubit to which the Hadamard gate was applied (here the third qubit). [2 marks]

(e) [6 marks] [New] Given the two terms - the phase-flip term and the bit-flip term - the error syndrome measurement will detect which qubit was bit-flipped

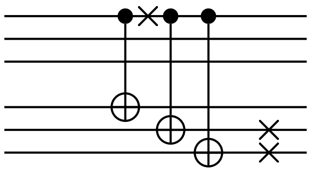
$$\begin{array}{lcll} (\alpha|\,100\,\rangle + \beta|\,011\,\rangle)|\,0\,\rangle|\,0\,\rangle & \mapsto & (\alpha|\,100\,\rangle + \beta|\,011\,\rangle)|\,1\,\rangle|\,0\,\rangle & \text{bit flip on 1st qubit} \\ (\alpha|\,010\,\rangle + \beta|\,101\,\rangle)|\,0\,\rangle|\,0\,\rangle & \mapsto & (\alpha|\,010\,\rangle + \beta|\,101\,\rangle)|\,1\,\rangle|\,1\,\rangle & \text{bit flip on 2nd qubit} \\ (\alpha|\,001\,\rangle + \beta|\,110\,\rangle)|\,0\,\rangle|\,0\,\rangle & \mapsto & (\alpha|\,001\,\rangle + \beta|\,110\,\rangle)|\,0\,\rangle|\,1\,\rangle & \text{bit flip on 3rd qubit} \end{array}$$

In either of these three cases the recovery operation is the bit-flip on the respected qubit. For example, outcome $x_1 = 0, x_2 = 1$ indicates that in order to recover the original state the bit-flip has to be applied to the third qubit. Unlike the familiar case of the three-qubit bit-flip error correcting code, the outcome $x_1 = 0, x_2 = 0$ does not indicate "no errors" but point to the first term (the phase-flip term)

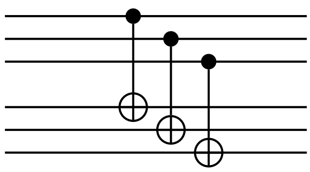
$$(\alpha|\,000\,\rangle - \beta|\,111\,\rangle)|\,0\,\rangle|\,0\,\rangle \mapsto (\alpha|\,000\,\rangle - \beta|\,111\,\rangle)|\,0\,\rangle|\,0\,\rangle.$$

Thus for outcome $x_1 = 0, x_2 = 0$ the recovery operation is the phase-flip on any of the three qubits, it does not matter which one.

(f) [5 marks] [New] Errors are unrecoverable if there is more than one error in each cluster of three qubits. In implementation A errors can propagate through the controlled-NOT gates. For example, if the first control qubit of the first controlled-NOT gate is bit-flipped (after the action of the gate), the two sub-sequent controlled-NOT gates will propagate the error and corrupt two qubits in the second cluster.



Implementation A



Implementation B

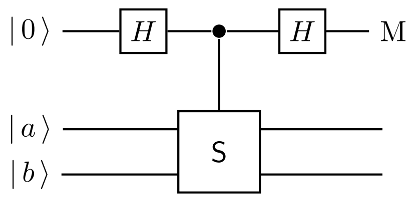
The probability of this to happen is p. In contrast, implementation B does not allow for error propagation and the probability of having two errors in a cluster if of the order of p^2. Implementation B is fault tolerant.

2. The swap gate S on two qubits is defined first on product vectors, $S : |\,a\,\rangle|\,b\,\rangle \mapsto |\,b\,\rangle|\,a\,\rangle$ and then extended to sums of products vectors by linearity.

   (a) [3 marks] Show that the four Bell states $\frac{1}{\sqrt{2}}(|\,00\,\rangle \pm |\,11\,\rangle)$, $\frac{1}{\sqrt{2}}(|\,01\,\rangle \pm |\,10\,\rangle)$ are eignevectors of S which form the orthonormal basis in the Hilbert space associated with two qubits. Which Bell states span the symmetric subspace (all eigenvectors of S with eigenvalue 1) and which the antisymmetric one (all eigenvectors of S with eigenvalue -1)? Can S have any other eigenvalues except ± 1?

   (b) [3 marks] Show that $P_{\pm} = \frac{1}{2}(\mathbb{1} \pm S)$ are two orthogonal projectors which form the decomposition of the identity and project on the symmetric and the antisymmetric subspaces. Decompose the state vector $|\,a\,\rangle|\,b\,\rangle$ of two qubits into symmetric and antisymmetric components.

   (c) [7 marks] Consider the following quantum network composed of the two Hadamard gates, one controlled-S operation (also known as the controlled-swap or the Fredkin gate) and the measurement M in the computational basis,



   The state vectors $|\,a\,\rangle$ and $|\,b\,\rangle$ are normalised but not orthogonal to each other. Step through the execution of this network, writing down quantum states of the three qubits after each computational step. What are the probabilities of observing 0 or 1 when the measurement M is performed?

   (d) [4 marks] Explain why this quantum network implements projections on the symmetric and the antisymmetric subspaces of the two qubits.

   (e) [4 marks] Two qubits are transmitted through a quantum channel which applies the same, randomly chosen, unitary operation U to each of them. Show that $U \otimes U$ leaves the symmetric and antisymmetric subspaces invariant.

   (f) [4 marks] Polarised photons are transmitted through an optical fibre. Due to the variation of the refractive index along the fibre the polarisation of each photon is rotated by the same unknown angle. This makes communication based on polarisation encoding unreliable. However, if you can prepare any polarisation state of two photons you can still use the channel and communicate without any errors. How can this be achieved?

SOLUTION TO QUESTION 2

(a) [3 marks] [New but based on standard material] Acting with S on each of the four Bell states gives us:

$$\begin{aligned} S\frac{|\,00\,\rangle \pm |\,11\,\rangle}{\sqrt{2}} &= \frac{|\,00\,\rangle \pm |\,11\,\rangle}{\sqrt{2}} \\ S\frac{|\,01\,\rangle + |\,10\,\rangle}{\sqrt{2}} &= \frac{|\,01\,\rangle + |\,10\,\rangle}{\sqrt{2}} \\ S\frac{|\,01\,\rangle - |\,10\,\rangle}{\sqrt{2}} &= -\frac{|\,01\,\rangle - |\,10\,\rangle}{\sqrt{2}}, \qquad \text{[1 mark]} \end{aligned}$$

from which we deduce that eigenvectors $\{\frac{1}{\sqrt{2}}(|\,00\,\rangle \pm |\,11\,\rangle), \frac{1}{\sqrt{2}}(|\,01\,\rangle + |\,10\,\rangle)\}$ span the three-dimensional symmetric subspace. The antisymmetric subspace is one-dimensional and spanned by $\frac{1}{\sqrt{2}}(|\,01\,\rangle - |\,10\,\rangle)$. [1 mark]

Since $S^2 = \mathbb{1}$, then S can only have two eigenvalues ± 1. [1 mark]

(b) [3 marks] [New but based on standard material] Again, using $S^2 = \mathbb{1}$, we get: $P_+P_- = 0$ and $P_\pm^2 = P_\pm$, which confirms that $P_\pm$ are orthogonal projectors. [2 marks]
Applying them to $|\,a\,\rangle|\,b\,\rangle$:

$$\begin{aligned} P_+(|\,a\,\rangle|\,b\,\rangle) &= \frac{1}{2}(|\,a\,\rangle|\,b\,\rangle) + |\,b\,\rangle|\,a\,\rangle) \\ P_-(|\,a\,\rangle|\,b\,\rangle) &= \frac{1}{2}(|\,a\,\rangle|\,b\,\rangle) - |\,b\,\rangle|\,a\,\rangle). \qquad \text{[1 mark]} \end{aligned}$$

(c) [7 marks] [New] Stepping through the network

$$\begin{aligned} |\,0\,\rangle|\,a\,\rangle|\,b\,\rangle &\mapsto \frac{1}{\sqrt{2}}(|\,0\,\rangle + |\,1\,\rangle)|\,a\,\rangle|\,b\,\rangle && (1) \\ &\mapsto \frac{1}{\sqrt{2}}(|\,0\,\rangle|\,a\,\rangle|\,b\,\rangle + |\,1\,\rangle|\,b\,\rangle|\,a\,\rangle) && (2) \\ &\mapsto \frac{1}{2}((|\,0\,\rangle + |\,1\,\rangle)|\,a\,\rangle|\,b\,\rangle + (|\,0\,\rangle - |\,1\,\rangle)|\,b\,\rangle|\,a\,\rangle) && (3) \\ &= |\,0\,\rangle\frac{1}{2}(|\,a\,\rangle|\,b\,\rangle + |\,b\,\rangle|\,a\,\rangle) + |\,1\,\rangle\frac{1}{2}(|\,a\,\rangle|\,b\,\rangle - |\,b\,\rangle|\,a\,\rangle). \qquad \text{[5 marks]} && (4) \end{aligned}$$

From the last expression we can see that the outcome 0 and 1 are observed with probabilities

$$\begin{aligned} \text{Probability of 0} &= \left|\frac{1}{2}(|\,a\,\rangle|\,b\,\rangle + |\,b\,\rangle|\,a\,\rangle)\right|^2 = \frac{1}{2}(1 + |\langle a|b\rangle|^2) \\ \text{Probability of 1} &= \left|\frac{1}{2}(|\,a\,\rangle|\,b\,\rangle - |\,b\,\rangle|\,a\,\rangle)\right|^2 = \frac{1}{2}(1 - |\langle a|b\rangle|^2) \qquad \text{[2 marks]} \end{aligned}$$

(d) [4 marks] [New but based on standard technique] The output state $|\,0\,\rangle \otimes \frac{1}{2}(|\,a\,\rangle|\,b\,\rangle + |\,b\,\rangle|\,a\,\rangle) + |\,1\,\rangle \otimes \frac{1}{2}(|\,a\,\rangle|\,b\,\rangle - |\,b\,\rangle|\,a\,\rangle)$ shows clearly that outcomes 0 or 1 lead to the "collapse" of the superposition to either the symmetric or the antisymmetric component of $|\,a\,\rangle|\,b\,\rangle$.

(e) [4 marks] [New] Operators S and $U \otimes U$ commute. $(U \otimes U)S|\,a\,\rangle|\,b\,\rangle = (U \otimes U)|\,b\,\rangle|\,a\,\rangle = |\,b'\,\rangle|\,a'\,\rangle$ and $S(U \otimes U)|\,a\,\rangle|\,b\,\rangle = S|\,a'\,\rangle|\,b'\,\rangle = |\,b'\,\rangle|\,a'\,\rangle$. Thus, the symmetric and the antisymmetric subspaces are invariant under the action of $U \otimes U$.

(f) [4 marks] Use symmetric and antisymmetric states to encode one bit of information. Here two photons are needed to encode one logical bit but the transmission is error free.

3. Any density matrix of a single qubit can be parametrised by the three real components of the Bloch vector $\vec{s} = (s_x, s_y, s_z)$ and written as

$$\varrho = \tfrac{1}{2}\left(\mathbb{1} + \vec{s}\cdot\vec{\sigma}\right),$$

where σ_x, σ_y and σ_z are the Pauli matrices, and $\vec{s}\cdot\vec{\sigma} = s_x\sigma_x + s_y\sigma_y + s_z\sigma_z$.

(a) [3 marks] Check that such parametrised ϱ has all the mathematical properties of a density matrix. Find the eigenvalues of ϱ and explain why the length of the Bloch vector cannot exceed 1.

(b) [5 marks] Any physically admissible operation on a qubit is described by a completely positive map which can always be written as

$$\varrho \mapsto \varrho' = \sum_k A_k \varrho A_k^\dagger$$

where matrices A_k satisfy $\sum_k A_k^\dagger A_k = \mathbb{1}$. Show that this map preserves positivity and trace. Show that any composition of completely positive maps is also completely positive.

(c) [9 marks] A qubit in state ϱ is transmitted through a depolarising channel that effects a completely positive map

$$\varrho \mapsto (1-p)\varrho + \frac{p}{3}\left(\sigma_x\varrho\sigma_x + \sigma_y\varrho\sigma_y + \sigma_z\varrho\sigma_z\right),$$

for some $0 \leqslant p \leqslant 1$. Show that under this map the Bloch vector associated with ϱ shrinks by the factor $(3-4p)/3$.

Consider a map $\mathcal{N}$, called universal-NOT, which acts on a single qubit and inverts its Bloch sphere,

$$\mathcal{N}(\mathbb{1}) = \mathbb{1} \quad \mathcal{N}(\sigma_x) = -\sigma_x \quad \mathcal{N}(\sigma_y) = -\sigma_y \quad \mathcal{N}(\sigma_z) = -\sigma_z$$

(d) [2 marks] Explain why $\mathcal{N}$, acting on a single qubit, maps density matrices to density matrices.

(e) [6 marks] The joint state of two qubits is described by the density matrix

$$\rho = \tfrac{1}{4}\left(\mathbb{1}\otimes\mathbb{1} + \sigma_x\otimes\sigma_x - \sigma_y\otimes\sigma_y + \sigma_z\otimes\sigma_z\right),$$

Apply $\mathcal{N}$ to the first qubit leaving the second qubit intact. Write the resulting matrix and explain why $\mathcal{N}$ is not a completely-positive map.

[*The Pauli matrices σ_x, σ_y, and σ_z are*

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}.$$

They anticommute and square to the identity $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = \mathbb{1}$.]

SOLUTION TO QUESTION 3

(a) [3 marks] [Bookwork] $\mathrm{Tr}\,\rho = \mathrm{Tr}\,{}^1\!/_2(\mathbb{1}+s_x\sigma_x+s_y\sigma_y+s_z\sigma_z) = \mathrm{Tr}\,{}^1\!/_2\mathbb{1} = 1$, because Pauli matrices have trace 0. The two eigenvalues of

$$\rho = \frac{1}{2}\begin{bmatrix} 1+s_z & s_x - i\,s_y \\ s_x + i\,s_y & 1-s_z \end{bmatrix}$$

are ${}^1\!/_2(1 \pm \sqrt{s_x^2+s_y^2+s_z^2}) = {}^1\!/_2(1 \pm |\vec{s}|)$ hence, for $\rho \geqslant 0$ we must require that $|\vec{s}| \leqslant 1$.

(b) [5 marks] For any vector $|\,v\,\rangle$ we can write $\langle\,v\,|\sum_k A_k\varrho A_k^\dagger|\,v\,\rangle$ as $\sum_k\langle\,v_k\,|\rho|\,v_k\,\rangle$ where $|\,v_k\,\rangle = A_k^\dagger|\,v\,\rangle$. We have $\langle\,v_k\,|\rho|\,v_k\,\rangle \geqslant 0$ for $\rho \geqslant 0$, hence $\langle\,v\,|\sum_k A_k\varrho A_k^\dagger|\,v\,\rangle \geqslant 0$ for any $|\,v\,\rangle$ which implies that $\rho' \geqslant 0$. [2 marks]

The trace is linear and cyclic thus $\mathrm{Tr}\left(\sum_k A_k\varrho A_k^\dagger\right) = \sum_k\left(\mathrm{Tr}\,A_k^\dagger A_k\varrho\right) = \mathrm{Tr}(\sum_k A_k^\dagger A_k)\varrho = \mathrm{Tr}\,\mathbb{1}\varrho = 1$ [1 mark]

Consider two completely positive maps described by the Kraus operators A_k and B_l. The composition $\sum_{k,l} B_l(A_k\varrho A_k^\dagger)B_l^\dagger = \sum_{k,l} B_lA_k\varrho(B_lA_k)^\dagger$ is a completely positive map with Kraus operators B_lA_k because $\sum_{k,l}(B_lA_k)^\dagger B_lA_k = \sum_k A_k^\dagger(\sum_l B_l^\dagger B_l)A_k = \mathbb{1}$. [2 marks]

(c) [9 marks] First observe that the Pauli operator anticommute, e.g. $\sigma_x\sigma_y\sigma_x = -\sigma_y$ and square to the identity, hence

$$\begin{aligned}
\sigma_x\,(\vec{s}\cdot\vec{\sigma})\,\sigma_x = \sigma_x\,(s_x\sigma_x+s_y\sigma_y+s_z\sigma_z)\,\sigma_x &= s_x\sigma_x - s_y\sigma_y - s_z\sigma_z,\\
\sigma_y\,(\vec{s}\cdot\vec{\sigma})\,\sigma_y = \sigma_y\,(s_x\sigma_x+s_y\sigma_y+s_z\sigma_z)\,\sigma_y &= s_y\sigma_y - s_x\sigma_x - s_z\sigma_z,\\
\sigma_z\,(\vec{s}\cdot\vec{\sigma})\,\sigma_z = \sigma_z\,(s_x\sigma_x+s_y\sigma_y+s_z\sigma_z)\,\sigma_z &= s_z\sigma_z - s_x\sigma_x - s_y\sigma_y.
\end{aligned}$$

This implies

$$\varrho \mapsto (1-p)\,\tfrac{1}{2}\,(\mathbb{1}+\vec{s}\cdot\vec{\sigma}) + p\,\tfrac{1}{2}\left(\mathbb{1}-\tfrac{1}{3}\vec{s}\cdot\vec{\sigma}\right) = \tfrac{1}{2}\left(\mathbb{1}+\tfrac{3-4p}{3}\,\vec{s}\cdot\vec{\sigma}\right).$$

(d) [2 marks] The map sends Bloch vector $\vec{s}$ to $-\vec{s}$, which is a legal Bloch vector parametrising a legal density matrix of a single qubit.

(e) [6 marks] Even though $\mathcal{N}$ maps density matrices to density matrices its extension $\mathcal{N}\otimes\mathbb{1}$ does not. It maps the density matrix (representing maximally entangled state $\frac{1}{\sqrt{2}}(|\,00\,\rangle+|\,11\,\rangle)$) to

$$\tfrac{1}{4}\,(\mathbb{1}\otimes\mathbb{1} - \sigma_x\otimes\sigma_x + \sigma_y\otimes\sigma_y - \sigma_z\otimes\sigma_z)\,,$$

which is not a density matrix for it is not positive semidefinite (one of the eigenvalues of this matrix is -1. One can see it, for example, by writing explicitly the resulting matrix in the computational basis

$$\frac{1}{2}\left[\begin{array}{c|cc|c} 0 & 0 & 0 & -1 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline -1 & 0 & 0 & 0 \end{array}\right]$$