Quantum Secret Sharing with Error Correction

Aziz Mouzali,1,* Fatiha Merazka,2 and Damian Markham3

1Electronic Department, National Polytechnic School, Algiers, Algeria
2Electronic and Computer Engineering Faculty, University of Science, and Technology Houari Boumediène, Algiers, Algeria
3Laboratoire Traitement et Communication de l’Information CNRS — Télécom ParisTech, France

(Received January 19, 2012; revised manuscript received May 22, 2012)

Abstract We investigate in this work a quantum error correction on a five-qubits graph state used for secret sharing through five noisy channels. We describe the procedure for the five, seven and nine qubits codes. It is known that the three codes always allow error recovery if only one among the sent qubits is disturbed in the transmitting channel. However, if two qubits and more are disturbed, then the correction will depend on the used code. We compare in this paper the three codes by computing the average fidelity between the sent secret and that measured by the receivers. We will treat the case where, at most, two qubits are affected in each one of five depolarizing channels.

PACS numbers: 03.67.Ac, 03.67.Hk, 03.67.Lx

Key words: quantum correction, graph state, quantum secret sharing, Feynman program

1 Introduction

The graph state can be very useful for several quantum protocols as secret sharing, measurement-based computation, error correction, teleportation and quantum communications. Then, it would be in the future a good way to unify these topics in one formalism. For example, an output of quantum computation considered as secret can be included in a graph state, then protected by a quantum error correcting code and sent through noisy channel to several receivers sharing this secret. The quantum secret sharing with graph state is very well described in Ref. [1], particularly the five qubits graph state. In this last case, only three receivers among five will access the secret, the two others being considered as eavesdroppers. In this work, we investigate the effects of the five, seven and nine qubits codes used to protect a five qubits graph state containing a secret and sent by a dealer to five players. We will compare the fidelity to determine the best code for a depolarizing channel where only one or two sent qubits are error affected. Some of the results have been obtained using a simulator called “Feynman Program”, which is a set of procedures supporting the definition and manipulation of an n-qubits system and the unitary gates acting on them. This program is described in details in Refs. [2–5].

2 Quantum Secret Sharing

Quantum secret sharing (QSS) is a quantum cryptographic protocol wherein a dealer shares private or public quantum channels with each player, while the players share private quantum or classical channels between each other. The dealer prepares an encoded version of the secret using a qubits string, which he transmits to n players, only a subset k of them can collaborate to reconstruct the secret. We call a (k, n) threshold secret sharing a protocol where each player receives one equal share of the encoded secret and a threshold of any k players can access the secret. This scheme is a primitive protocol by which any other secret sharing is achieved. In this work, we treated the case (k, n) = (3, 5) where the dealer sends through five depolarizing channels, a quantum secret encoded in a five qubits graph state.[1]

2.1 Introduction to Graph State

Graph states are an efficient tool for multipartite quantum information processing task like secret sharing. Also, they have a graphical representation which offers an intuitive picture of information flow. The secret to be shared is encoded onto classical labels placed on vertices of the graph representing local operations. The entanglement of the graph state allows these labels to be shifted around, giving us the opportunity to see graphically which set of players can access the secret.[1]

2.2 Five-Qubit Graph State

The five qubits graph state |G⟩ given by Eq. (1) is schematized in Fig. 1 where the vertices represent the qubits and the edges the controlled-Z gate. The graph state |ΨG⟩ given by Eq. (2) and containing the quantum secret |Ψs⟩ = α|0⟩ + β|1⟩ = cos(θ/2)|0⟩ + e^iφ sin(θ/2)|1⟩, should be transmitted by a dealer to five players through five different channels. First, he constructs the state |G⟩ from an initial five qubits state |Ψ0⟩ = |00000⟩, then applies the Hadamard gate H on each qubit and the controlled-Z gate CZ on qubits [1, 2], [2, 3], [3, 4], [4, 5], [5, 1].
The secret should be accessible only for players 1, 2, and 3, players 4 and 5 being considered as eavesdroppers. Players 1 and 3 measure their qubits in the Bell basis and transmit the result to player 2 which applies on its qubit the suitable recovering gate $R_g$ given in Table 1 to access the secret state.\[1\]

We describe below this procedure. Equation (4a) can be written:

$$\begin{align*}
|\Psi_G\rangle &= |B_{00}\rangle_{13}|\Psi_a\rangle_{245} + |B_{01}\rangle_{13}|\Psi_b\rangle_{245} \\
&\quad + |B_{10}\rangle_{13}|\Psi_c\rangle_{245} + |B_{11}\rangle_{13}|\Psi_d\rangle_{245},
\end{align*}$$

(5a)

where

$$\begin{align*}
|\Psi_a\rangle_{245} &= \frac{1}{2}(|\alpha\rangle + |\beta\rangle)_2 |B_{01}\rangle_{45}, \\
|\Psi_b\rangle_{245} &= \frac{1}{2}(|\alpha\rangle - |\beta\rangle)_2 |B_{10}\rangle_{45}, \\
|\Psi_c\rangle_{245} &= \frac{1}{2}(|\alpha\rangle - |\beta\rangle)_2 |B_{00}\rangle_{45}, \\
|\Psi_d\rangle_{245} &= \frac{1}{2}(|\alpha\rangle + |\beta\rangle)_2 |B_{11}\rangle_{45}.
\end{align*}$$

(5b)

Measurement in the Bell base $\{|B_{ij}\rangle_{13}\}$ gives only one term of the superposition in Eq. (5a), then the global density matrix:

$$\rho_{1,...,5} = \frac{\langle B_{ij}\rangle\langle B_{ij}\rangle_{13} \langle\Psi_x\rangle \langle\Psi_x\rangle_{245}}{4}$$

$$= \frac{\langle\rho_{ij}\rangle_{13} \langle\rho_x\rangle_{245}}{4},$$

(6)

with $x = a, b, c$ or $d$.

The partial trace over qubits (4,5) gives the density matrix of qubit 2:

$$\rho'_2 = \langle\Psi_2\rangle = P_{tr}(\langle\rho_x\rangle_{245}|4,5).$$

(7)

Then the secret state:

$$\rho_2 = R_g\rho'_2R_g^\dagger$$

or $|\Psi_2\rangle = R_g|\Psi'_2\rangle$.

(8)

### Table 1

| $|B_{ij}\rangle_{13}$ | $B_{00}$ | $B_{01}$ | $B_{10}$ | $B_{11}$ |
|---------------------|-------|-------|-------|-------|
| $R_g$               | H     | ZH    | ZXH   | XH    |

### 2.4 Bit and Phase Flip

The sent qubits can be affected by error $X$, $Z$ or $Y$ represented respectively by the Pauli matrix

$$X = \begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix}, \quad Z = \begin{pmatrix}
1 & 0 \\
0 & -1
\end{pmatrix},$$

$$Y = -iXZ = i \begin{pmatrix}
0 & -1 \\
1 & 0
\end{pmatrix},$$

corresponding to rotation $\pi$ around ox or oz or both in the block sphere. We have applied the procedure described in Subsec. 2.3 and have obtained Table 2 giving the affected secret state $|\Psi^E\rangle_2$.

### Table 2

| Error | $|\Psi^E\rangle_2$ |
|-------|------------------|
| $X_1, X_2, Y_2$ | $\alpha|1\rangle - \beta|0\rangle$ |
| $Z_1, X_2, Z_3$ | $\alpha|0\rangle - \beta|1\rangle$ |
| $Z_2, Y_1, Y_3$ | $\alpha|1\rangle + \beta|0\rangle$ |
2.5 Fidelity

The fidelity is one of the mathematical quantities which permits to know how close are two quantum states represented by the density matrix $\sigma$ and $\rho$ by measuring a distance between them: [6]

$$F(\sigma, \rho) = \left| \text{Tr} \left( \sqrt{\sigma \rho \sqrt{\sigma} \rho} \right) \right|^2.$$  \hfill (9)

In the case of a pure state $|\Psi\rangle = |\Psi\rangle \langle \Psi|$ and an arbitrary state $\rho$, the fidelity is the overlap between the two states: [6]

$$F(|\Psi\rangle, \rho) = \langle \Psi | \rho | \Psi \rangle.$$  \hfill (10)

In this work we measure the overlap between the correct secret state $\sigma = |\Psi_u\rangle \langle \Psi_u|$ and the qubit state $\rho_2 = |\Psi_2\rangle \langle \Psi_2|$ measured by player 2 to access the secret. Then, the fidelity is function of the angles $(\theta, \phi)$ in the Bloch sphere and the average fidelity is:

$$F_a = (1/4\pi) \int \int F(\theta, \phi) \sin(\theta) \, d\theta \, d\phi,$$  \hfill (11)

with $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$.

We will describe below the procedure giving the fidelity. If any Pauli errors $E = \sigma_0$, $\sigma_x$, $\sigma_y$ or $\sigma_z$ affect the state $|\Psi_G\rangle$ in the transmission channel, we can see from Eq. (4a) that Eq. (5a) will keep the same form and become:

$$|\Psi'_G\rangle = |B_{00}\rangle_{13} |\Psi'_{E_1}\rangle_{1245} + |B_{01}\rangle_{13} |\Psi'_{E_2}\rangle_{1245} + |B_{10}\rangle_{13} |\Psi'_{E_3}\rangle_{1245} + |B_{11}\rangle_{13} |\Psi'_{E_4}\rangle_{1245},$$  \hfill (12)

where $|\Psi'_{E_{a,b,c,d}}\rangle_{1245}$ are the new global states of qubits system $(2,4,5)$ modified by the channel errors.

We note that $|\Psi'_{E_{a,b,c,d}}\rangle_{1245} \neq E|\Psi_{a,b,c,d}\rangle_{1245}$ as channel error can affect qubits $(1,3)$ as well as qubits $(2,4,5)$. In fact, if an error affects qubits $(1,3)$ or $(4,5)$, then their global state will simply change to another Bell state. Similarly, if qubit 2 is affected, then its state will only switch to one of the forms appearing in Eq. (4a).

After measuring on the Bell states of qubits $(1,3)$ only one term will remain in Eq. (12):

$$|\Psi'_{G}\rangle = \left( \frac{1}{2} \right) |B_{ij}\rangle_{13} |\Psi'_{E}\rangle_{1245}.$$  \hfill (13)

The corresponding affected density matrix is:

$$\rho'_{1,...,5} = \left( \frac{1}{4} \right) (|B_{ij}\rangle \langle B_{ij}|)_{13} (|\Psi'_{E}\rangle \langle \Psi'_{E}|)_{1245} = \rho_{1,...,5} \left( \frac{1}{4} \right) (|\rho_{ij}\rangle \langle \rho_{ij}|)_{13} (|\rho_{E}\rangle \langle \rho_{E}|)_{245}.$$  \hfill (14)

The partial trace over qubits $(4,5)$ gives the measured density matrix of qubit 2:

$$\rho_2' = |\Psi'_{G}\rangle \langle \Psi'_{G}| = \text{Tr}_{13} (|\rho_{E}\rangle \langle \rho_{E}|)_{245}.  \hfill (15)$$

Then the affected secret state measured by player two:

$$\rho_2' = R_{G} \rho_2 \text{Tr}_{245} |\Psi'_{E}\rangle \langle \Psi'_{E}|.$$  \hfill (16)

We multiply by the secret state $|\Psi_u\rangle = \alpha |0\rangle + \beta |1\rangle$ to obtain the fidelity:

$$F(\theta, \phi) = \langle \Psi_u | \rho_2' | \Psi_u \rangle.$$  \hfill (17)

Table 3 gives the fidelity $F(\theta, \phi)$ calculated by Feynman program for all the errors on qubits $i = 1,2$ or 3. Figure 2 shows the fidelity $F(\theta, \phi_0 = 0$ or $\pi/2$) function of the angle $\theta$ for error occurring with probability $P = 1$ on one, two and three noisy channels. We note for example that if $|\Psi_s\rangle = (\sqrt{2}/2) (|0\rangle + |1\rangle)$ the fidelity is the best $(F_a = 1)$ for error $X_1$ and the worst $(F_a = 0)$ for error $Z_1$. Also, we deduce from Eq. (4) that any errors on qubits 4 and 5 do not affect the secret state giving then fidelity equal to one.

Fig. 2 Fidelity $F(\theta, \phi)$ with $0 < \theta < \pi$, $\phi = \pi/2$ for errors $\epsilon_a$ and $\phi = 0$ for errors $\epsilon_c$. We note that for errors $\epsilon_d$ we have $F(\theta, \phi) = 1$ for $0 < \theta, \phi < \pi$.

Table 3 Fidelity and measured state $|\Psi_2\rangle$ versus errors on qubits $i = 1,2,3$. The error groups are depicted on Table 4.

| Error | $|\Psi_2\rangle$ | $F(\theta, \phi)$ | $F_a$ |
|-------|----------------|-----------------|------|
| $\epsilon_a$ | $\alpha|1\rangle - \beta|0\rangle$ | $|\sin(\theta) \sin(\phi)|^2$ | $1/3$ |
| $\epsilon_b$ | $\alpha|0\rangle - \beta|1\rangle$ | $\cos^2(\theta)$ | $1/3$ |
| $\epsilon_c$ | $\alpha|1\rangle + \beta|0\rangle$ | $|\sin(\theta) \cos(\phi)|^2$ | $1/3$ |
| $\epsilon_d$ | $\alpha|0\rangle + \beta|1\rangle$ | $1$ | $1$ |

2.6 Depolarizing Channel

The depolarizing channel is a particular model for the noise on quantum systems. In this process, the global density matrix $\rho$ is replaced by a mixed one $\rho(P)$ function of the probability $P$ that a Pauli error $E_{ij} = (\sigma_{ij} = \sigma_x, \sigma_y, \sigma_z = \sigma_z)$ or $\sigma_{ij} = \sigma_{ij}$ affects any qubit “$j$” in the $n$-qubits system. For one-qubit system the matrix density is given by Eq. (18)[2] and for the $n$-qubits system it can be generalized by Eq. (19):

$$\rho_1(P) = (1 - P) \rho + \frac{P}{3} [X \rho X + Y \rho Y + Z \rho Z], \hfill (18)$$

$$\rho_n(P) = (1 - P)^n \rho + \cdots + \frac{P^n}{3^n} (1 - P)^{n-k} \times \sum_{1 \leq i \leq n} (\Pi_{1 \leq l \leq k} \sigma_{ij}^l) \rho(\Pi_{1 \leq l \leq k} \sigma_{ij}^l) + \cdots + \frac{P^n}{3^n} \sum_{1 \leq i \leq n} (\Pi_{1 \leq l \leq n} \sigma_{ij}^l) \rho(\Pi_{1 \leq l \leq n} \sigma_{ij}^l). \hfill (19)$$
Consider now the case where the five qubits are sent by the dealer through five depolarizing channels. Suppose the probability $P$ that any single error occurs on any qubit is the same in the five channels. Then we can use Eq. (19) as if the dealer sends the five qubits through only one depolarized channel. We describe below the procedure to obtain the average fidelity $F_a(P)$, considering all the possible errors in the five transmitting noisy channels. We begin by writing the affected density matrix $\rho_1^{5}(P)$ received by the five players:

$$
\rho_1^{5}(P) = (1 - P)^5 \rho_{1} + \frac{P}{3} (1 - P)^4 
\times \left[ \rho_{1} + \rho_{2} + \rho_{3} + \rho_{4} + \rho_{5} \right] 
+ \rho_{1}^{5} + \rho_{1}^{2} \rho_{2} + \rho_{1}^{2} \rho_{3} + \rho_{1}^{2} \rho_{4} + \rho_{1}^{2} \rho_{5} 
+ \rho_{1} \rho_{2} \rho_{3} + \rho_{1} \rho_{2} \rho_{4} + \rho_{1} \rho_{2} \rho_{5} 
+ \rho_{1} \rho_{3} \rho_{4} + \rho_{1} \rho_{3} \rho_{5} + \rho_{1} \rho_{4} \rho_{5} + \rho_{2} \rho_{3} \rho_{4} + \rho_{2} \rho_{3} \rho_{5} + \rho_{2} \rho_{4} \rho_{5} + \rho_{3} \rho_{4} \rho_{5}.
$$

With $\rho_1^{5}$ the density matrix affected by errors on qubit $a$:

$$
\rho_1^{5} = X_1 \rho_{1} + Y_1 \rho_{1} + Z_1 \rho_{1} + Z_1 \rho_{1}.
$$

The density matrix $\rho_{1}, \rho_{2}, \rho_{3}, \rho_{4}, \rho_{5}$ are summation of respectively 9, 27, 81, and 243 terms and represent the density matrix affected by error on two, three, four and five qubits.

After measuring on the Bell states of qubits (1, 3) we obtain:

$$
\rho_{245}^{2}(P) = (1 - P)^5 \rho_{245} + \frac{P}{3} (1 - P)^4 
\times \left[ \rho_{1} + \rho_{2} + \rho_{3} + \rho_{4} + \rho_{5} \right] 
+ \rho_{1} \rho_{2} \rho_{3} + \rho_{1} \rho_{2} \rho_{4} + \rho_{1} \rho_{2} \rho_{5} 
+ \rho_{1} \rho_{3} \rho_{4} + \rho_{1} \rho_{3} \rho_{5} + \rho_{1} \rho_{4} \rho_{5} + \rho_{2} \rho_{3} \rho_{4} + \rho_{2} \rho_{3} \rho_{5} + \rho_{2} \rho_{4} \rho_{5} 
+ \rho_{3} \rho_{4} \rho_{5}.
$$

With $\rho_{245}^{2} = (\rho_{a}^{245}, \rho_{b}^{245}, \rho_{c}^{245})$ or $\rho_{d}^{245}$ and $\rho_{245}^{2} = (\rho_{a}^{245}, \rho_{b}^{245}, \rho_{c}^{245}, \rho_{d}^{245})$.

After tracing over qubits (4, 5) and multiplying by the recovering gate $R_g$ we obtain:

$$
\rho_{2}^{2}(P) = (1 - P)^5 \rho_{2} + \frac{P}{3} (1 - P)^4 
\times \left[ \rho_{1} + \rho_{2} + \rho_{3} + \rho_{4} + \rho_{5} \right] 
+ \rho_{1} \rho_{2} \rho_{3} + \rho_{1} \rho_{2} \rho_{4} + \rho_{1} \rho_{2} \rho_{5} 
+ \rho_{1} \rho_{3} \rho_{4} + \rho_{1} \rho_{3} \rho_{5} + \rho_{1} \rho_{4} \rho_{5} + \rho_{2} \rho_{3} \rho_{4} + \rho_{2} \rho_{3} \rho_{5} + \rho_{2} \rho_{4} \rho_{5} 
+ \rho_{3} \rho_{4} \rho_{5}.
$$

With $\rho_{2}^{2} = (\rho_{a}^{2}, \rho_{b}^{2}, \rho_{c}^{2})$ or $\rho_{d}^{2}$ or $\rho_{e}^{2}$ the secret state disturbed by error $E = E_1, E_2, E_3, E_4, E_5, E_6, E_7, E_8, E_9, E_{10}, E_{11}, E_{12}$, or $E_1, E_2, E_3, E_4, E_5$.

We multiply by the secret state and integrate over $(\theta, \phi)$ to obtain the average fidelity:

$$
\langle \Psi_s | \rho_{2}^{2} | \Psi_s \rangle = (1 - P)^5 + \frac{P}{3} (1 - P)^4 
\times \left[ \rho_{1} + \rho_{2} + \rho_{3} + \rho_{4} + \rho_{5} \right] 
+ \rho_{1} \rho_{2} \rho_{3} + \rho_{1} \rho_{2} \rho_{4} + \rho_{1} \rho_{2} \rho_{5} 
+ \rho_{1} \rho_{3} \rho_{4} + \rho_{1} \rho_{3} \rho_{5} + \rho_{1} \rho_{4} \rho_{5} + \rho_{2} \rho_{3} \rho_{4} + \rho_{2} \rho_{3} \rho_{5} + \rho_{2} \rho_{4} \rho_{5} 
+ \rho_{3} \rho_{4} \rho_{5}.
$$

With $\langle \Psi_s | \rho_{2} | \Psi_s \rangle = 1$, and $F_a^{\rho_{2}} = \langle \Psi_s | \rho_{2} | \Psi_s \rangle$.

We can write Eq. (24) as

$$
\langle \Psi_s | \rho_{2}^{2} | \Psi_s \rangle = (1 - P)^5 + \frac{P}{3} (1 - P)^4 |A| + \frac{P^2}{9} (1 - P)^3 |B|
+ \frac{P^3}{27} (1 - P)^2 |C| + \frac{P^4}{81} (1 - P)^4 |D| + \frac{P^5}{243} |E|.
$$

We deduce from Tables 3 and 4 the values of $F_a^{\rho_{2}}$ contained in Table 5:
The dealer protects each of the three qubits (1, 2, 3) with four ancillas as showed in Fig. 3 and sends them through three noisy channels, which introduce a bit or phase flip or both with probability \( P = 1 \).

The graph state (3) can be written as follow:

\[
|\Psi_G\rangle = (\sqrt{2}/8)[\{\alpha|0\rangle + \beta|1\rangle]|\Psi_a\rangle_{jklm} \\
+ [\alpha|0\rangle - \beta|1\rangle]|\Psi_b\rangle_{jklm} \\
+ [\beta|0\rangle + \alpha|1\rangle]|\Psi_c\rangle_{jklm} \\
+ [\beta|0\rangle - \alpha|1\rangle]|\Psi_d\rangle_{jklm}].
\]

With

\[
[i = 1, (j, k, l, m) = 2, 3, 4, 5], \\
i = 2, (j, k, l, m) = 1, 3, 4, 5 \\
or \ i = 3, (j, k, l, m) = 1, 2, 4, 5.
\]
The states $|\Psi_i\rangle_{jklm}$, $|\Psi_j\rangle_{jklm}$, $|\Psi_k\rangle_{jklm}$, $|\Psi_l\rangle_{jklm}$ have different expressions depending on the value of “i”. We suppose that the dealer knows that the secret will be accessed by players (1, 2, 3). Then he will not protect the qubits sent to players (4, 5) as the channel errors on them do not affect the accessed secret. To protect qubit “i” the dealer adds four ancillas each one in the state $|0\rangle$. After applying the coding circuit we obtain the coded graph state $|\Psi_{G_i}\rangle$ sent by the dealer, where $|0\rangle$ and $|1\rangle$ are the logical qubits:

$$|\Psi_{G_i}\rangle = (\sqrt{2}/8)(|\alpha(0)\rangle + |\beta(1)\rangle)|\Psi_i\rangle_{jklm} + |\alpha(0)\rangle - |\beta(1)\rangle)|\Psi_j\rangle_{jklm} + |\beta(0)\rangle - |\alpha(1)\rangle)|\Psi_k\rangle_{jklm} + |\beta(0)\rangle - |\alpha(1)\rangle)|\Psi_l\rangle_{jklm}.$$  \hspace{1cm} (32)

After syndrome measurement, correction and decoding, the players suppress the ancillas. If the qubit “i” is affected by error $E_i = X_i, Y_i$ or $Z_i$ then the graph state becomes:

$$|\Psi_{G_i}^c\rangle = E_i|\Psi_{G_i}\rangle = (\sqrt{2}/8)(|\alpha(0)\rangle + |\beta(1)\rangle)|\Psi_i\rangle_{jklm} + E_i(|\alpha(0)\rangle - |\beta(1)\rangle)|\Psi_j\rangle_{jklm} + E_i(|\beta(0)\rangle - |\alpha(1)\rangle)|\Psi_k\rangle_{jklm} + E_i(|\beta(0)\rangle - |\alpha(1)\rangle)|\Psi_l\rangle_{jklm}.$$ \hspace{1cm} (33)

Table 6 gives the syndromes $S$ for the five qubits code of single and double errors occurring in the logical qubit “i”. The double errors are corrected as the single error having same syndrome. The third column gives the error $E_i$ affecting the to be protected physical qubit “i” after decoding obtained by Feynman Program.

| Error | $S$ | $E_i$ |
|-------|-----|-------|
| $X_{i1}, (Z_{a2} Z_{a3})$, $(X_{a3} Z_{a4}, Z_{a4} X_{a2})$ | 001 | $Z_i$ |
| $X_{i2}, (Z_{a2} Z_{a3})$, $(Z_{a2} X_{a3}, Z_{a2} X_{a3})$ | 001 | $Z_i$ |
| $X_{i2}, (Z_{a2} Z_{a3})$, $(X_{a3} Z_{a4}, Z_{a4} X_{a4})$ | 100 | $X_i$ |
| $X_{i3}, (Z_{a2} Z_{a3})$, $(X_{a2} X_{a4}, Z_{a3} X_{a4})$ | 100 | $X_i$ |
| $X_{i4}, (X_{a2} Z_{a3})$, $(X_{a3} Z_{a4}, Z_{a2} X_{a3})$ | 100 | $X_i$ |
| $Y_{i1}, (X_{a2} X_{a3}, Z_{a4})$ | 110 | $I_i$ |
| $Y_{i1}, (X_{a2} X_{a4}, Z_{a2} Z_{a4})$ | 110 | $I_i$ |
| $Y_{i2}, (X_{a3} X_{a4}, Z_{a3} X_{a4})$ | 110 | $I_i$ |
| $Y_{i3}, (X_{a2} X_{a4}, Z_{a2} Z_{a4})$ | 011 | $I_i$ |
| $Y_{i4}$ | 101 | $I_i$ |

### 3.2 Depolarizing Channel

Consider three double errors $E_k E_i, E_m E_n$ and $E_o E_p$ occurring respectively in channels “1”, “2”, and “3” on any qubits ($k, l, m, n, o, p$) and corrected as the single error with similar syndrome. The qubits (4, 5) are not protected and can be affected by any error $X, Y$ or $Z$. If the probability that channel error occurs on one qubit is equal to $P$, then the density matrix received by the five players is:

$$\rho^{(123a)(45)} = (1 - P)^8 \rho^{(123a)(45)} + \frac{P}{3}(1 - P)^7 \left[ \sum \rho^{E_i(123a)(45)} + \frac{P^2}{3^2}(1 - P)^6 \left[ \sum \rho^{E_i(123a)(45)} \right] \right]$$

$$+ \frac{P^3}{3^3}(1 - P)^5 \left[ \sum \rho^{E_i E_j(123a)(45)} \right] + \frac{P^4}{3^4}(1 - P)^4 \left[ \sum \rho^{E_i E_j E_k(123a)(45)} \right] + \frac{P^5}{3^5}(1 - P)^3 \left[ \sum \rho^{E_i E_j E_k E_l(123a)(45)} \right]$$

$$+ \frac{P^7}{3^7}(1 - P)^2 \left[ \sum \rho^{E_i E_j E_k E_l E_m(123a)(45)} \right] + \frac{P^8}{3^8}(1 - P)^1 \left[ \sum \rho^{E_i E_j E_k E_l E_m E_n(123a)(45)} \right].$$ \hspace{1cm} (34)

The notation (123a) represents the logical qubits 1, 2, and 3, each one protected by four ancillas and:

$$\sum \rho^{E_i} = \rho^{E_i(123a)(45)} + \rho^{E_i(132a)(45)} + \rho^{E_m} + \rho^{E_o} + \rho^{E_p} + \rho^{E_x} + \rho^{E_y} + \rho^{E_z}.$$ \hspace{1cm} (35a)

$$\rho^{E_i(123a)(45)} = \rho^{E_i(123a)(45)} + \rho^{E_i(132a)(45)} + \rho^{E_i(123a)(45)} + \rho^{E_i(123a)(45)} + \rho^{E_i(123a)(45)} + \rho^{E_i(123a)(45)} + \rho^{E_i(123a)(45)} + \rho^{E_i(123a)(45)}.$$ \hspace{1cm} (35b)

The summations $\sum \rho^{E_i(123a)(45)}$, $\sum \rho^{E_i E_j(123a)(45)}$, $\sum \rho^{E_i E_j E_k(123a)(45)}$, $\sum \rho^{E_i E_j E_k E_l(123a)(45)}$, $\sum \rho^{E_i E_j E_k E_l E_m(123a)(45)}$, $\sum \rho^{E_i E_j E_k E_l E_m E_n(123a)(45)}$, and $\sum \rho^{E_i E_j E_k E_l E_m E_n E_o E_p E_q E_r E_s E_t E_u}$ contain respectively 8X3, 28X3, 56X3, 70X3, 56X3, 28X3, 8X3, and 8X3 terms. The expression $\rho^{(123a)(45)}$ is the summation of $3^6$ terms.

After decoding and suppressing the ancillas we obtain by using Tables 6 the affected graph state:

$$\rho^{(1,...,5)} = \left[ (1 - P)^8 + 18 \frac{P}{3}(1 - P)^7 + 108 \frac{P^2}{9}(1 - P)^6 + 216 \frac{P^3}{27}(1 - P)^5 \right] \rho^{(1,...,5)}$$

$$+ \left[ 3 \frac{P^2}{9}(1 - P)^6 + 36 \frac{P^3}{27}(1 - P)^5 + 108 \frac{P^4}{81}(1 - P)^4 \right] \rho^{E_1(1,...,5)} + \rho^{E_2(1,...,5)} + \rho^{E_3(1,...,5)}$$

$$+ \left[ 9 \frac{P^4}{81}(1 - P)^4 + 54 \frac{P^5}{243}(1 - P)^3 \right] \rho^{E_1 E_2(1,...,5)} + \rho^{E_1 E_3(1,...,5)} + \rho^{E_2 E_3(1,...,5)} + \left[ \frac{1}{27} P^6(1 - P)^2 \right] \rho^{E_1 E_2 E_3(1,...,5)}.$$
We deduce from Table 5:

\[ F_a(P) = \langle \Psi_s | \rho_a^2 | \Psi_s \rangle = \left[ (1 - P)^8 + 18 \frac{P^2}{3} (1 - P)^7 + 108 \frac{P^4}{27} (1 - P)^6 + 216 \frac{P^6}{81} (1 - P)^5 \right] \\
+ \left[ \frac{P^2}{9} (1 - P)^6 + 36 \frac{P^3}{27} (1 - P)^5 + 108 \frac{P^4}{81} (1 - P)^4 \right] [F_{E_1} + F_{E_2} + F_{E_3}] \\
+ \left[ 9 \frac{P^4}{81} (1 - P)^4 + 54 \frac{P^5}{243} (1 - P)^3 \right] [F_{E_1} E_2 E_3 + F_{E_1} E_2 E_4 + F_{E_1} E_2 E_5 + F_{E_1} E_3 E_4 + F_{E_1} E_3 E_5 + F_{E_1} E_4 E_5] \\
\times \left[ \frac{P^2}{3} (1 - P)^7 + 18 \frac{P^2}{9} (1 - P)^6 + 108 \frac{P^3}{27} (1 - P)^5 + 216 \frac{P^4}{81} (1 - P)^4 \right] [F_{E_1} + F_{E_3}] \\
+ \left[ \frac{P^2}{9} (1 - P)^6 + 18 \frac{P^3}{27} (1 - P)^5 + 108 \frac{P^4}{81} (1 - P)^4 \right] [F_{E_1} E_3] \\
+ \left[ 3 \frac{P^3}{27} (1 - P)^5 + 36 \frac{P^4}{81} (1 - P)^4 + 108 \frac{P^5}{243} (1 - P)^3 \right] [F_{E_1} E_4 E_5 + F_{E_1} E_3 E_4 + F_{E_1} E_3 E_5 + F_{E_1} E_4 E_5] \\
+ \left[ 3 \frac{P^4}{81} (1 - P)^4 + 36 \frac{P^5}{243} (1 - P)^3 \right] [F_{E_1} E_2 E_3 E_4 + F_{E_1} E_2 E_3 E_5 + F_{E_1} E_2 E_4 E_5 + F_{E_1} E_2 E_3 E_5 + F_{E_1} E_2 E_4 E_5 + F_{E_1} E_2 E_3 E_5] \\
+ \left[ 9 \frac{P^5}{243} (1 - P)^2 + 54 \frac{P^6}{36} (1 - P) \right] [F_{E_1} E_2 E_3 E_4 + F_{E_1} E_2 E_3 E_5 + F_{E_1} E_2 E_4 E_5 + F_{E_1} E_2 E_3 E_5 + F_{E_1} E_2 E_4 E_5 + F_{E_1} E_2 E_3 E_5] \\
+ \left[ 27 \frac{P^7}{36} (1 - P) \right] [F_{E_1} E_2 E_3 E_4 E_5 + F_{E_1} E_2 E_3 E_4 E_5 + F_{E_1} E_2 E_3 E_4 E_5 + F_{E_1} E_2 E_3 E_4 E_5 + F_{E_1} E_2 E_3 E_4 E_5 + F_{E_1} E_2 E_3 E_4 E_5]. \]
Then:

\[
F_a(P) = (1 - P)^8 + 8P(1 - P)^7 + 26P^2(1 - P)^6 + 44P^3(1 - P)^5 + \frac{128}{3}P^4(1 - P)^4 \\
+ \frac{80}{3}P^5(1 - P)^3 + \frac{346}{27}P^6(1 - P)^2 + \frac{116}{27}P^7(1 - P) + \frac{13}{27}P^8.
\]

(39)

4 The Seven-Qubit Code

This code is described in Ref. [8] and uses five qubits to protect one of them against an \( X, Y \) or \( Z \) error. Tables 7–9 depict the error \( E_i \) on the protected qubit “\( i \)" (after correction) for different channel errors \( E \).

| \( E \) | \( S \) | \( E_i \) | \( E \) | \( S \) | \( E_i \) |
|---|---|---|---|---|---|
| \( X_1, (X_2X_3, X_4X_5, X_6X_7) \) | 000001 | \( I_i, (X_i) \) | \( Y_1 \) | 001001 | \( I_i \) |
| \( X_2, (X_1X_3, X_4X_6, X_5X_7) \) | 000100 | \( I_i, (X_i) \) | \( Y_2 \) | 010001 | \( I_i \) |
| \( X_3, (X_1X_2, X_3X_4, X_5X_7) \) | 000111 | \( I_i, (X_i) \) | \( Y_3 \) | 011011 | \( I_i \) |
| \( X_4, (X_1X_5, X_2X_6, X_3X_7) \) | 001000 | \( I_i, (X_i) \) | \( Y_4 \) | 100100 | \( I_i \) |
| \( X_5, (X_1X_4, X_2X_7, X_3X_6) \) | 001011 | \( I_i, (X_i) \) | \( Y_5 \) | 101101 | \( I_i \) |
| \( X_6, (X_1X_7, X_2X_4, X_3X_5) \) | 001110 | \( I_i, (X_i) \) | \( Y_6 \) | 110110 | \( I_i \) |
| \( X_7, (X_1X_6, X_2X_5, X_3X_4) \) | 001111 | \( I_i, (X_i) \) | \( Y_7 \) | 111111 | \( I_i \) |

**Table 7** Syndromes and the error \( E_i \) affecting the protected qubits “\( i \)" after correction by an operators \( X_k \) or \( Y_k \) (\( k = 1, \ldots, 7 \)).

| Errors | \( S \) | \( E_i \) |
|---|---|---|
| \( Z_1, (Z_2Z_6, Z_7Z_3, Z_1Z_5) \) | 001000 | \( I_i, (Z_i) \) |
| \( Z_2, (Z_1Z_7, Z_5Z_6, Z_2Z_7) \) | 010000 | \( I_i, (Z_i) \) |
| \( Z_3, (Z_1Z_2, Z_7Z_3, Z_2Z_6) \) | 011000 | \( I_i, (Z_i) \) |
| \( Z_4, (Z_1Z_2, Z_7Z_5, Z_2Z_6) \) | 100000 | \( I_i, (Z_i) \) |
| \( Z_5, (Z_1Z_2, Z_5Z_4, Z_3Z_6) \) | 101000 | \( I_i, (Z_i) \) |
| \( Z_6, (Z_1Z_2, Z_3Z_4, Z_1Z_3) \) | 110000 | \( I_i, (Z_i) \) |
| \( Z_7, (Z_1Z_6, Z_2Z_3, Z_1Z_4) \) | 111000 | \( I_i, (Z_i) \) |

**Table 8** Syndromes and the error affecting the protected qubits after correction by an operator \( Z_k \) (\( k = 1, \ldots, 7 \)).

| Errors | \( S \) | \( E_i \) |
|---|---|---|
| \( X_1Z_4 \) | 100001 | \( Z_1X_4 \) |
| \( X_1Z_5 \) | 101001 | \( Z_2X_4 \) |
| \( X_1Z_6 \) | 110001 | \( Z_3X_4 \) |
| \( X_1Z_7 \) | 111001 | \( Z_4X_4 \) |
| \( X_2Z_4 \) | 100111 | \( Z_1X_5 \) |
| \( X_2Z_5 \) | 110111 | \( Z_2X_5 \) |
| \( X_2Z_6 \) | 111101 | \( Z_3X_5 \) |
| \( X_2Z_7 \) | 111111 | \( Z_4X_5 \) |
| \( X_3Z_4 \) | 101111 | \( Z_1X_6 \) |
| \( X_3Z_5 \) | 111011 | \( Z_2X_6 \) |
| \( X_3Z_6 \) | 111111 | \( Z_3X_6 \) |
| \( X_3Z_7 \) | 111110 | \( Z_4X_6 \) |

**Table 9** Syndromes of double channels errors \( Z_kX_1 \) not affecting the protected qubits after correction.

| Errors | \( S \) | Errors | \( S \) | Errors | \( S \) |
|---|---|---|---|---|---|
| \( X_1Z_4 \) | 100001 | \( Z_1X_4 \) | 001001 | \( Z_2X_4 \) | 001010 |
| \( X_1Z_5 \) | 101001 | \( Z_2X_4 \) | 010100 | \( X_1Z_2 \) | 010001 |
| \( X_1Z_6 \) | 110001 | \( Z_3X_4 \) | 011100 | \( X_1Z_3 \) | 011001 |
| \( X_1Z_7 \) | 111001 | \( Z_4X_4 \) | 001101 | \( X_2Z_1 \) | 001010 |
| \( X_2Z_4 \) | 100111 | \( Z_1X_5 \) | 001101 | \( X_2Z_2 \) | 010100 |
| \( X_2Z_5 \) | 110111 | \( Z_2X_5 \) | 010101 | \( X_2Z_3 \) | 011010 |
| \( X_2Z_6 \) | 111011 | \( Z_3X_5 \) | 011110 | \( X_2Z_4 \) | 011010 |
| \( X_2Z_7 \) | 111111 | \( Z_4X_5 \) | 001111 | \( Z_2X_3 \) | 010001 |
| \( X_3Z_4 \) | 101111 | \( Z_1X_6 \) | 011111 | \( Z_3X_3 \) | 010001 |
| \( X_3Z_5 \) | 111011 | \( Z_2X_6 \) | 011111 | \( Z_4X_3 \) | 010001 |
| \( X_3Z_6 \) | 111111 | \( Z_3X_6 \) | 011111 | \( Z_2X_4 \) | 010001 |

5 The Nine-Qubit Code

This code called the Shor code and explained in Ref. [6] uses nine qubits to protect one of them in a superposed state from any error \( X, Y \) or \( Z \). The simulation with Feynman Program gives in Tables 10–14 the error \( E_i \) affecting the protected qubits (after correction) for different single and double channels errors \( E \) on logical qubit “\( i \)".
Table 10  Syndromes $S$ and the $E_i$ error affecting the protected qubits after correction by an operators $X_k$ ($k = 1, \ldots, 9$).

| $E$            | $S$         | $E_i$ |
|---------------|-------------|-------|
| $Y_1, X_1 Z_{2,3}$ | 10000010    | $I_i$ |
| $Y_2, X_2 Z_{1,3}$ | 11000010    | $I_i$ |
| $Y_3, X_3 Z_{1,2}$ | 01000010    | $I_i$ |
| $Y_4, X_4 Z_{5,6}$ | 00100011    | $I_i$ |
| $Y_5, X_5 Z_{4,6}$ | 00100111    | $I_i$ |
| $Y_6, X_6 Z_{4,5}$ | 00010011    | $I_i$ |
| $Y_7, X_7 Z_{8,9}$ | 00001001    | $I_i$ |
| $Y_8, X_8 Z_{7,9}$ | 00001101    | $I_i$ |
| $Y_9, X_9 Z_{7,8}$ | 00000101    | $I_i$ |

Table 11  Syndromes $S$ and the $E_i$ affecting the protected qubits after correction by an operators $Y_k$ ($k = 1, \ldots, 9$).

| $E$            | $S$         | $E_i$ |
|---------------|-------------|-------|
| $Y_1, X_1 Z_{2,3}$ | 10000010    | $I_i$ |
| $Y_2, X_2 Z_{1,3}$ | 11000010    | $I_i$ |
| $Y_3, X_3 Z_{1,2}$ | 01000010    | $I_i$ |
| $Y_4, X_4 Z_{5,6}$ | 00100011    | $I_i$ |
| $Y_5, X_5 Z_{4,6}$ | 00100111    | $I_i$ |
| $Y_6, X_6 Z_{4,5}$ | 00010011    | $I_i$ |
| $Y_7, X_7 Z_{8,9}$ | 00001001    | $I_i$ |
| $Y_8, X_8 Z_{7,9}$ | 00001101    | $I_i$ |
| $Y_9, X_9 Z_{7,8}$ | 00000101    | $I_i$ |

Table 12  Syndromes $S$ and the $E_i$ affecting the protected qubits after correction by an operator $Z_k$ ($k = 1, \ldots, 9$).

| Errors                                   | $S$         | $E_i$ |
|------------------------------------------|-------------|-------|
| $(Z_1, Z_2, Z_3), (Z_4 Z_{7,8,9}, Z_5 Z_{7,8,9}, Z_6 Z_{7,8,9})$ | 00000010    | $(I_i), (X_i)$ |
| $(Z_4, Z_5, Z_6), (Z_1 Z_{7,8,9}, Z_2 Z_{7,8,9}, Z_3 Z_{7,8,9})$ | 00000011    | $(I_i), (X_i)$ |
| $(Z_7, Z_8, Z_9), (Z_1 Z_{4,5,6}, Z_2 Z_{4,5,6}, Z_3 Z_{4,5,6})$ | 00000001    | $(I_i), (X_i)$ |
| $(Z_1 Z_{2,3}, Z_2 Z_3, Z_4 Z_{5,6}, Z_5 Z_6, Z_7 Z_{8,9}, Z_8 Z_9)$ | 00000000    | $(I_i)$ |

Table 13  Syndromes $S$ of double channels errors $X_k X_l$ not affecting the protected qubits after correction.

| $E$       | $S$         | $E$       | $S$         | $E$       | $S$         |
|-----------|-------------|-----------|-------------|-----------|-------------|
| $X_1 X_4$ | 10100000    | $X_2 X_7$ | 11001000    | $X_4 X_7$ | 00101000    |
| $X_1 X_5$ | 10110000    | $X_2 X_8$ | 11001100    | $X_4 X_8$ | 00101100    |
| $X_1 X_6$ | 10010000    | $X_3 X_9$ | 11000100    | $X_4 X_9$ | 00100100    |
| $X_1 X_7$ | 10001000    | $X_3 X_4$ | 01100000    | $X_5 X_7$ | 00111000    |
| $X_1 X_8$ | 10001100    | $X_3 X_5$ | 01110000    | $X_5 X_8$ | 00111100    |
| $X_1 X_9$ | 10000100    | $X_3 X_6$ | 01010000    | $X_5 X_9$ | 00110100    |
| $X_2 X_4$ | 11100000    | $X_3 X_7$ | 01001000    | $X_6 X_7$ | 00011000    |
| $X_2 X_5$ | 11110000    | $X_3 X_8$ | 01001100    | $X_6 X_8$ | 00011100    |
| $X_2 X_6$ | 11010000    | $X_3 X_9$ | 01000100    | $X_6 X_9$ | 00010100    |
The difference comes from the number Sec. 4 is the same for the seven and nine qubits codes.

| E | S | E | S |
|---|---|---|---|
| X1Z_{4,5,6} | 10000001 | X4Z_{1,2,3} | 00100010 |
| X1Z_{7,8,9} | 10000001 | X5Z_{1,2,3} | 00110010 |
| X2Z_{7,8,9} | 11000001 | X6Z_{1,2,3} | 00010010 |
| X2Z_{4,5,6} | 11000001 | X7Z_{1,2,3} | 00001010 |
| X3Z_{4,5,6} | 01000011 | X8Z_{1,2,3} | 00001110 |
| X3Z_{7,8,9} | 01000001 | X9Z_{1,2,3} | 00000110 |
| X4Z_{7,8,9} | 00100001 | X10Z_{1,2,3} | 00000111 |
| X5Z_{7,8,9} | 00100001 | X11Z_{1,2,3} | 00000111 |
| X6Z_{7,8,9} | 00010001 | X12Z_{1,2,3} | 00000111 |

6 Comparison Among the Three Codes

The procedure giving the average fidelity described in Sec. 4 is the same for the seven and nine qubits codes. The difference comes from the number n of double channel errors having an exclusive syndrome allowing their recovery, then letting the protected qubit error free. We suppose that triple channel errors and more are very unlikely. We deduce from Tables 6–14 and for each code the next fractions of recoverable double channel errors:

\[ \frac{n_5}{N_5} = 0, \quad \frac{n_7}{N_7} = \frac{39}{81}, \quad \frac{n_9}{N_9} = \frac{108}{144}. \]  \hfill (40)

With \( N_5=40, N_7=81, \) and \( N_9=144 \) the total number of double errors for each code. We can deduce the average fidelity by changing the value \( f_a = 1/3 \) in Table 3 by an average value \( f_n \) and obtain for each code:

\[ f_5 \equiv \frac{1}{3}, \quad f_7 = \frac{(n_7 \times 1 + (N_7 - n_7) \times 1/3)}{81} = \frac{53}{81}, \]

\[ f_9 = \frac{(n_9 \times 1 + (N_9 - n_9) \times 1/3)}{144} = \frac{5}{6} . \]  \hfill (41)

We substitute in Table 5 the value 1/3 by the average value \( f_n \) (except in the last arrow as for \( P = 1 \) the errors are unrecoverable whatever is the code). Equation (39) becomes:

\[
F_a(P) = \langle \Psi_s | \rho_s^2 | \Psi_s \rangle = \left[ (1 - P)^8 + 18 \frac{P}{3} (1 - P)^7 + 108 \frac{P^2}{9} (1 - P)^6 + 216 \frac{P^3}{27} (1 - P)^5 \right] + \left[ 3 \frac{P^2}{9} (1 - P)^6 + 30 \frac{P^3}{27} (1 - P)^5 + 108 \frac{P^4}{81} (1 - P)^4 \right] + \left[ 9 \frac{P^4}{81} (1 - P)^4 + 54 \frac{P^5}{243} (1 - P)^3 \right] + \left[ 3 \frac{P^5}{27} (1 - P)^5 \right] + \left[ 36 \frac{P^4}{81} (1 - P)^4 + 108 \frac{P^5}{243} (1 - P)^3 \right] + \left[ 54 \frac{P^6}{36} (1 - P)^2 \right] + \left[ 9 \frac{P^6}{36} (1 - P)^2 + 54 \frac{P^7}{27} (1 - P) \right] + \left[ 27 \frac{P^7}{3} (1 - P) \right].
\]  \hfill (42)

We obtain:

\[
F_a(P) = (1 - P)^8 + 8P(1 - P)^7 + 3(3f_n + 25)2P^2(1 - P)^6 + (18f_n + 38)3P^3(1 - P)^5 + (41f_n + 29)4P^4 \times (1 - P)^4 + (44f_n + 12)5P^5(1 - P)^3 + (205f_n + 47)6P^6(1 - P)^2 + (50f_n + 22)7P^7(1 - P) + \frac{13}{27}P^8. \]  \hfill (43)

7 Summary

Table 15 summarizes all the results and Fig. 4 compares the average fidelity without and with correction by the three codes. Figure 1 shows logically that the average fidelity is decreasing with P without and with correction by any code. The values of fidelity are always better and the decrease is slower when using codes. The best average fidelity is given by the nine qubits code, followed by the seven qubits then the five qubits code. The reason is that for the five qubits code all the double errors (in logical qubit) let the protected qubits affected, while some of them could be covered when using the two other codes.

![Fig. 4](image-url) (Color online) Fidelity without and with correction by the five, seven and nine qubits codes.
We consider in this work that triple errors (in logical qubits) and more are very unlikely, so that syndrome measurement allows (in seven and nine qubits code) recovering errors. We note that if \( P = 1 \), then the average fidelity \( F_a(P = 1) = 13/27 = 0.4815 \) is the same regardless the used code.

### Table 15
Fidelity without and with correction by the five, seven and nine qubits codes. The symbol \( C_0 \) corresponds to no correction.

| Code | \( F_a(P) \) |
|------|-------------|
| \( C_0 \) | \( 1 - 2P + \frac{8}{3}P^2 - \frac{32}{27}P^3 \) |
| \( C_n \) | \( (1 - P)^8 + 8P(1 - P)^7 + (3f_n + 25)P^2(1 - P)^6 + (18f_n + 38)P^3(1 - P)^5 + (41f_n + 29)P^4(1 - P)^4 \) |
| \( C_n \) | \( +(44f_n + 12)P^5(1 - P)^3 + \left(\frac{205f_n + 47}{9}\right)P^6(1 - P)^2 + \left(\frac{50f_n + 22}{9}\right)P^7(1 - P)^1 + \frac{13}{27}P^8 \) |
| \( C_5 \) | \( (1 - P)^8 + 8P(1 - P)^7 + 26P^2(1 - P)^6 + 44P^3(1 - P)^5 + \frac{128}{3}P^4(1 - P)^4 \) |
| \( C_7 \) | \( \frac{80}{3}P^5(1 - P)^3 + \frac{346}{27}P^6(1 - P)^2 + \frac{116}{27}P^7(1 - P)^1 + \frac{13}{27}P^8 \) |
| \( C_9 \) | \( (1 - P)^8 + 8P(1 - P)^7 + 72P^2(1 - P)^6 + 448P^3(1 - P)^5 + \frac{4522}{3}P^4(1 - P)^4 \) |
| \( C_9 \) | \( \frac{3304}{81}P^5(1 - P)^3 + \frac{14672}{279}P^6(1 - P)^2 + \frac{4432}{279}P^7(1 - P)^1 + \frac{13}{27}P^8 \) |
| \( C_9 \) | \( (1 - P)^8 + 8P(1 - P)^7 + \frac{55}{2}P^2(1 - P)^6 + 53P^3(1 - P)^5 + \frac{378}{6}P^4(1 - P)^4 \) |
| \( C_9 \) | \( \frac{146}{3}P^5(1 - P)^3 + \frac{1307}{54}P^6(1 - P)^2 + \frac{191}{27}P^7(1 - P)^1 + \frac{13}{27}P^8 \) |

### 8 Conclusion

This work was devoted to error correction for quantum secret sharing. The results show that the nine qubits code gives the best fidelity, followed by the seven, then the five qubits code, regardless the depolarizing channel error probability \( P \). This conclusion seems to confirm the simulation work done in Ref. \cite{9} where errors were introduced by the correction process itself. We conclude that higher is the ancillas number better is the fidelity. The reason is that the nine qubits code offers a higher fraction of double channel errors letting unaffected the received useful qubit. In fact, as only single and double errors have been considered, the nine qubits code gives a specific syndrome for a higher number of double errors, then allowing their recovery which lead to fidelity equal to one. We have supposed that triple errors and more are very unlikely and then with negligible effect on the obtained results.

### Acknowledgments

We would like to thank very much Mrs. S. Fritzsch and T. Radtke for providing us with the version 4 (2008) of Feynman Program.

### References

[1] Damian Markham and Barry C. Sanders, Phys. Rev. A \textbf{78} (2008) 042309.
[2] T. Radtke and S. Fritzsch, Compt. Phys. Commun. \textbf{173} (2005) 91.
[3] T. Radtke and S. Fritzsch, Compt. Phys. Commun. \textbf{175} (2006) 145.
[4] T. Radtke and S. Fritzsch, Compt. Phys. Commun. \textbf{176} (2007) 617.
[5] T. Radtke and S Fritzsch, Compt. Phys. Commun. \textbf{179} (2008) 647.
[6] M.A. Nielsen and I.L. Chuang, \textit{Quantum Computation and Information}, Cambridge University Press, Cambridge (2000).
[7] Raymond Laflamme, \textit{et al.}, Phys. Rev. Lett. \textbf{77} (1996) 198.
[8] A.M. Steane, Proc. R. Soc. Lond. A \textbf{452} (1996) 2551, quant-ph/9601029.
[9] Jumpei Niwa, Keiji Matsumoto, and Hiroshi Imai, \textit{Simulating the Effects of Quantum Error-correction Schemes}, arXiv:quant-ph/0211071v1, 13 Nov. (2002).