COMP-649A 2005 Homework set #4

This HW counts for half the value of the others
Due Tuesday December 13, 2005

A. Purity testing codes

Consider the following Purity testing protocol (to purify $|\Psi^-\rangle^{\otimes n}$ states) :

Construction 2 (Simple Random Hashing Protocol)

1. *Alice picks $2n$ random bits $x_1,\ldots,x_n,z_1,\ldots,z_n$ such that not all the bits are 0.*
2. *Alice will measure the operator given by $X^{x_1}Z^{z_1}\otimes\cdots\otimes X^{x_n}Z^{z_n}$. To do this Alice:*
   (a) *Considers only qubits where $(x_i,z_i)\neq(0,0)$. Say there remain ℓ qubits.*
   (b) *On qubit j, applies either*
   $H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$ *if* $(x_j,z_j)=(0,1)$,
   $B=\frac{1}{\sqrt{2}}\begin{pmatrix}1&i\\i&1\end{pmatrix}$ *if* $(x_j,z_j)=(1,1)$,
   the identity if $(x_j,z_j)=(1,0)$.
   (c) *Applies C-NOT from each of the first $\ell-1$ qubits onto the last.*
   (d) *Measures the last in the computational basis.*
   (e) *Applies the inverse transformation to the remaining qubits.*
3. *Alice sends $x_1,\ldots,x_n,z_1,\ldots,z_n$ and her measurement result to Bob.*
4. *Bob performs the same measurement and sends back the result.*
5. *Alice and Bob accept if the two results are different and reject otherwise.*

Remember definition 3 from the paper of Barnum, Crépeau, Gottesman, Smith, Tapp for *stabilizer purity testing codes*:

Definition 3 *A stabilizer purity testing code with error* ϵ *is a set of stabilizer codes* $\{Q_k\}$*, for* $k \in \mathcal{K}$*, such that* $\forall E_x \in E$ *with* $x \neq 0$*,* $\#\{k | x \in Q_k^{\perp} - Q_k\} \leq \epsilon(\#\mathcal{K})$.

That is, for any error x in the error group, if k is chosen later at random, the probability that the code Q_k detects x is at least $1 - \epsilon$.

a) Observe that the previous protocol defines at *step 1* a random stabilizer code of dimension *n-1* and prove that the set of all stabilizer codes of dimension *n-1* is a *stabilizer purity testing code* with error *1/2*.
(Consider the error space *E*={ Pauli errors on *n* qubits}.)

b) Inspired by the above question, prove that the set of all stabilizer codes of dimension *n-s* is a *stabilizer purity testing code* with error 2^{-s}.
(Consider the error space *E*={ Pauli errors on *n* qubits}.)

c) Explicit the number of bits necessary to share the description of a random stabilizer code of dimension *n-s.* Explicit the number of shared secret bits necessary to implement a parity testing protocol that uses the code of b) in the context of quantum authentication (where no interaction is desired).