COMP-649A 2005 Homework set #2

Due Tuesday October 25, 2005 in class at 14h35

Observations on observables

Definition : An observable is an hermitien operator $\mathcal{O}$ such that, if its spectral decomposition into projector is $\mathcal{O} = \sum_i \lambda_i P_i$, then $\sum_i P_i = \mathbb{I}$.

Question #1 (6 points)

Let operator R_1 be defined as $Z_1 \otimes \mathbb{I}_2$ and R_2 be defined as $\mathbb{I}_1 \otimes Z_2$. Proof that $R_1 \cdot R_2 \neq Z_1 \otimes Z_2$. Think of $R_1 \cdot R_2$ as a circuit, first applying R_2 and getting an eigenvalue and then applying R_1 and getting a new eigenvalue, whilst $Z_1 \otimes Z_2$ is a single operator that returns a single eigenvalue.

Question #2 (6 points)

Show that nevertheless they give the same statistics — i.e. if one multiply the output of R_1 and R_2, then that single output will be distributed just as the output of $Z_1 \otimes Z_2$.

Lengthy introduction : Approximate quantum encryption defines a cypher $\mathcal{E}$ to be secure if for all density operator ρ the following criterion is satisfied $\|\mathcal{E}(\rho) - \mathbb{I}/d\|_\alpha < \epsilon$, where alpha specifies a norm. So intuitively any measurement made on $\mathcal{E}(\rho)$ should have statistics similar to the same measurement applied to $\mathbb{I}$.

Let the bias of a random variable A be defined as $|\Pr[A = 0] - \Pr[\mathrm{A} = 1]|$. We say a variable is ϵ-biased if its bias is inferior to ϵ.

Question #3 (18 points)

Let Π_i be a Pauli operator in a space of dimension that fits $\mathcal{E}(\rho)$. Prove that

1. $|\mathrm{tr}(\Pi_i \mathcal{E}(\rho))|$ is the bias of the Π_i observable applied to $\mathcal{E}(\rho)$.
2. if $\mathcal{E}$ is an approximate encryption scheme for the trace norm, then $\Pi_i \mathcal{E}(\rho)$ is ϵ-biased.

Stabilizer codes

Question #4 (6 points)

Read pages 454 to 464 in Nielsen & Chuang and solve problem 10.42

Question #5 (12 points)

Read section 10.5.5 and 10.5.8 (and 10.5.6 for your benefit) and solve problem 12.34 on page 597.

Quantum Forney Codes – Zyablov bound

Question #6 (6 points)

Show that the dual of a Reed-Solomon code of parameters $[N, K, D = N - K + 1]$ is a Generalized Reed-Solomon code of parameters $[N, N - K, D = K + 1]$.

Question #7 (12 points)

Exhibit how we may use the CSS construction to produce Quantum Reed-Solomon codes of parameters $[[N, K' = 2K - N, D' = N - K + 1]]$. In the light of the no-cloning theorem, explain why it is not surprizing that $K' > 0$ iff $D' \leq N/2$.

Question #8 (16 points)

Show that we can pick random linear binary codes C_1, C_2, such that $C_2^{\perp} \subset C_1$, both with parameters $[n, k > (1/2 + \epsilon)n, d > \alpha n]$, for $\epsilon, \alpha > 0$. Show that indeed we can do this as long as $\epsilon \leq 1/2 - h(\alpha)$ which is on the (classical) Varshamov-Gilbert bound. Conclude that we can produce binary quantum CSS codes of parameters $[[n, (1 - 2h(\delta))n, \delta n]]$, $0 < \delta < h^{-1}(1/2)$. Compare this result with the Quantum Varshamov-Gilbert bound.

You may choose to solve any one of the following two questions.
If you solve both we'll give you extra credit. But don't go mad trying to solve this whole assignment...

Question #9 (18 points)

Show how we can concatenate Quantum Reed-Solomon codes over $\mathbb{F}_{2^m}$ and inner random binary linear codes as above to obtain a family of $[[N \in O(m(2^m - 1)), \rho N, \delta N]]$ binary quantum codes such that $\rho, \delta > 0$. Maximize simultaneously the parameters $\rho, \delta > 0$ and plot the corresponding curve relating them. You have established the Quantum (weak) Zyablov bound.

Oberserve that these codes can be efficiently (as a function of N) constructed, encoded and decoded (upto $\delta N/4$). Justify this observation.

Question #10 (18 points)

In contrast, the Quantum (strong) Zyablov bound would be obtained by concatenating Quantum Reed-Solomon codes over $\mathbb{F}_{2^m}$ with inner random codes on the (Quantum) Varshamov-Gilbert bound to obtain a family of $[[N \in O(m(2^m - 1)), \rho N, \delta N]]$ binary quantum codes such that $\rho, \delta > 0$. Again, maximize simultaneously the parameters $\rho, \delta > 0$ and plot the corresponding curve relating them.

What can you say about efficiently (as a function of N) constructing, encoding and decoding (upto $\delta N/4$) these codes?

1 Reed-Solomon Codes

1.1 definition

A Reed-Solomon Code (RS) over $\mathbb{F}_q$ is a BCH code of length $N = q - 1$.

The dimension of such a code is $K = N - deg(g) = N - \delta + 1$ and its minimal distance is

$$D = \delta = N - K + 1.$$

Théorème 1.1 (interpolation de Lagrange) *Let $\alpha^{i_1}\alpha^{i_2}...\alpha^{i_K}$ be distincts elements of $\mathbb{F}_q$ for $K < q$ and $\beta_1\beta_2...\beta_K$ be any elements of $\mathbb{F}_q$. There exists a unique polynomial $p(x)$ over $\mathbb{F}_q$ such that $deg(p) < K$ and that for $1 \leq j < K$*

$$p(\alpha^{i_j}) = \beta_i.$$

Théorème 1.2 *Consider the code defined by*

$$C = \{(p(1)p(\alpha)...p(\alpha^{N-1})) : p \textit{ is a polynomial of degree } < K \textit{ over } \mathbb{F}_q\}.$$

The code C is an $[N = q - 1, K, N - K + 1]$ RS code .

Proof: first, it is clear that the dimension of C is K because there are q^K polynomials p of degree $< K$. The minimum distance is deduced by observing that $p \neq p'$ implies that $(p(1)p(\alpha)...p(\alpha^{N-1})) \neq (p'(1)p'(\alpha)...p'(\alpha^{N-1}))$ on at least $N - K + 1$ positions. Let p and p' be two polynomials such that

$$\Delta\left((p(1)p(\alpha)...p(\alpha^{N-1}), (p'(1)p'(\alpha)...p'(\alpha^{N-1})\right) < N - K + 1.$$

This implies that there exist $i_1, i_2, ..., i_K$ such that $p(\alpha^{i_j}) = p'(\alpha^{i_j})$. By the theorem "d'interpolation de Lagrange" we get $p = p'$. Therefore, there does not exist distinct c, c' such that $\Delta(c, c') < N - K + 1$.

2 Concatenated Codes

2.1 concatenation of codes

A concatenated code C is obtained from an *external* code C_E over $\mathbb{F}_{q^m}$ with parameters $[n_E, k_E, d_E]$ and an *internal* code C_I over $\mathbb{F}_q$ with parameters $[n_I, k_I = m, d_I]$. The result of concatenation is a code over $\mathbb{F}_q$ with parameters $[n = n_E n_I, k = k_E k_I = m k_E, d = d_E d_I]$.

2.2 internal random or maximal codes

If we construct concatenated codes using a Reed-Solomon external code with parameters $[2^m, R2^m, (1-R)2^m+1]$ and an internal binary code with parameters $[\sigma m, m, \rho m]$, near the V-G bound ($1/\sigma \approx 1 - h(\rho/\sigma)$) we obtain concatenated codes with parameters $[\sigma m 2^m, Rm2^m, (1-R)\rho m 2^m]$. Let $N = \sigma m 2^m$, $r = \frac{1}{\sigma}$ and substituting for ρ we obtain

$$[N, RrN, (1-R)h^{-1}(1-r)N].$$

If we fix the product $\gamma = Rr$, we may look for the r which maximises $(1-\frac{\gamma}{r})h^{-1}(1-r)$ to obtain the best codes of this type.

We may find internal codes by sampling random $\sigma m \times m$ binary matrices until we find one such that the minimum distance of the related code is close enough to the V-G bound.

3 Generalized Reed-Solomon Codes

A Generalized Reed-Solomon code (GRS) over $\mathbb{F}_{q^m}^N$ is caracterised by two vectors $\vec{\alpha}, \vec{v}$ of length N with $\vec{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_N) \in \mathbb{F}_{q^m}^N$ for distinct α_i and $\vec{v} = (v_1, v_2, ..., v_N) \in (\mathbb{F}_{q^m} \backslash \{\vec{0}\})^N$. The codewords are obtained from polynomials F of degree $< K$ by

$$c = (c_1 c_2 ... c_N) = (v_1 F(\alpha_1), v_2 F(\alpha_2), ..., v_N F(\alpha_N)).$$

3.1 the dual of a GRS code is a GRS code

To each $GRS(\vec{\alpha}, \vec{v})$ code of dimension K we associate another $GRS(\vec{\alpha}, \vec{v}')$ of dimension $N-K$ dual to the former. This means that the parity check matrix of such a $GRS(\vec{\alpha}, \vec{v}')$ code is of the form

$$\vec{H} = \begin{bmatrix} v'_1 & v'_2 & ... & v'_N \\ v'_1\alpha_1 & v'_2\alpha_2 & ... & v'_N\alpha_N \\ \vdots & \vdots & \ddots & \vdots \\ v'_1\alpha_1^{N-K-1} & v'_2\alpha_2^{N-K-1} & ... & v'_N\alpha_N^{N-K-1} \end{bmatrix}.$$