COMP-649A 2005 Homework set #2

Due Thursday October 20, 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 (5 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 (5 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 (15 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 $|\mathrm{tr}(\Pi_i \mathcal{E}(\rho))|$ is ϵ-biased.

Stabilizer codes

Question #4 (5 points)

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

Question #5 (10 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 (5 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 (10 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 $D' > N/2$.

Question #8 (15 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.

Question #9 (15 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 (15 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 Codes Reed-Solomon

1.1 definition

Un code Reed-Solomon (RS) sur $\mathbb{F}_q$ est un code BCH de longueur $N = q - 1$.

La dimension d'un tel code est $K = N - deg(g) = N - \delta + 1$ et sa distance minimale est

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

Théorème 1.1 (interpolation de Lagrange) *Soit $\alpha^{i_1}\alpha^{i_2}...\alpha^{i_K}$ des éléments distincts de $\mathbb{F}_q$ pour $K < q$ et $\beta_1\beta_2...\beta_K$ des éléments quelconques de $\mathbb{F}_q$. Il existe un unique polynôme $p(x)$ sur $\mathbb{F}_q$ tel que $deg(p) < K$ et que pour $1 \leq j < K$*

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

Théorème 1.2 *Consiérons le code définit ainsi*

$$C = \{(p(1)p(\alpha)...p(\alpha^{N-1})) : p \text{ est un polynôme de degré} < K \text{ sur } \mathbb{F}_q\}.$$

Le code C est un RS code $[N = q - 1, K, N - K + 1]$.

Preuve: d'abord il est clair que la dimension de C est K car il existe q^K valeurs de p et $p \neq p'$ implique que $(p(1)p(\alpha)...p(\alpha^{N-1})) \neq (p'(1)p'(\alpha)...p'(\alpha^{N-1}))$. Soient p et p' deux polynômes tels que

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

Ceci implique qu'ils existent $i_1, i_2, ..., i_K$ tels que $p(\alpha^{i_j}) = p'(\alpha^{i_j})$. Par le théoreme d'interpolation de Lagrange ceci entraîne que $p = p'$. Donc il n'existe pas de pair c, c' de mots distincts tels que $\Delta(c, c') < N - K + 1$.

2 Codes Concaténés

2.1 concaténation de codes

Un code concaténé C est obtenu à partir de deux codes C_E dit *externe* sur $\mathbb{F}_{q^m}$ de paramètres $[n_E, k_E, d_E]$ et C_I dit *interne* sur $\mathbb{F}_q$ de paramètres $[n_I, k_I = m, d_I]$. Le code ainsi obtenu sera un code sur $\mathbb{F}_q$ de paramètres $[n = n_E n_I, k = k_E k_I = m k_E, d = d_E d_I]$.

2.2 code interne aléatoire ou maximal

Si l'on construit des codes concaténés en prenant comme code externe un Reed-Solomon $[2^m, R2^m, (1-R)2^m+1]$ et comme code binaire interne $[\sigma m, m, \rho m]$ un code près de la borne de V-G ($1/\sigma \approx 1 - h(\rho/\sigma)$) on obtiendra des codes concaténés de paramètres $[\sigma m 2^m, Rm2^m, (1-R)\rho m 2^m]$. En posant $N = \sigma m 2^m$, $r = \frac{1}{\sigma}$ et en éliminant ρ on obtient

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

Si l'on fixe le produit $\gamma = Rr$ il faudra prendre le r qui maximise l'expression suivante $(1 - \frac{\gamma}{r})h^{-1}(1-r)$ pour obtenir les meilleurs codes de ce type.

On peut trouver les codes internes en prenant des matrices aléatoires de taille $\sigma m \times m$ jsuqu'à ce que l'on en trouve une dont la distance minimale associée soit assez près de la borne de V-G.

3 Codes Reed-Solomon généralisés

Un code Reed-Solomon Généralisé (RSG) sur $\mathbb{F}_{q^m}^N$ est caractérisé par deux vecteurs $\vec{\alpha}, \vec{v}$ de longueur N avec $\vec{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_N) \in \mathbb{F}_{q^m}^N$ pour des α_i distincts et $\vec{v} = (v_1, v_2, ..., v_N) \in (\mathbb{F}_{q^m} \backslash \{\vec{0}\})^N$. Les mots d'un tel code sont obtenus à partir des polynômes F de degré $< K$ par

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

3.1 le dual d'un code RSG est RSG

À chaque $RSG(\vec{\alpha}, \vec{v})$ de dimension K on peut associer un autre $RSG(\vec{\alpha}, \vec{v}')$ de dimension $N-K$ dual au premier. Ceci veut dire que la matrice de parité d'un code $RSG(\vec{\alpha}, \vec{v}')$ est donnée par

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