Some constructions of maximal witness codes

Bertrand MEYER

Télécom ParisTech

Aachen, August 25th 2011

Progression

Witness codes

Definition

- *A code $\mathcal{C}$ is a subset of $\mathbb{F}_2^n$.*
- *A witness of a codeword c is a set of coordinates $W \subseteq [n]$ such that on the restriction*

$$\forall c' \neq c \in \mathcal{C}, \qquad c_{|W} \neq c'_{|W}.$$

- *A w-witness code $\mathcal{C}$ is a code with witnesses of length $\leqslant w$.*

Example : A 2-witness code of length 6 with 4 codewords

$$\mathcal{C} = \left\{ \begin{array}{l} \boxed{1\ 0}\,0\ 1\ 0\ 1\ , \\ \boxed{0}\,0\ 0\ 1\ 0\,\boxed{0}, \\ 1\ 1\ 0\,\boxed{1\ 1}\,0\ , \\ 0\,\boxed{0}\,1\ 0\,\boxed{1}\,1 \end{array} \right\}.$$

State of the art

Our question

What is $f(n, w) = \max |\mathcal{C}|$?

where $\mathcal{C}$ is a w-witness code of length n.

Example : The Hamming sphere $\mathcal{S}_n(w)$ of radius w is a w-witness code. So

$$\binom{n}{w} \leqslant f(n, w).$$

Theorem (Cohen, Randriam, Zémor, 08)

For any fixed w, the sequence $n \mapsto f(n, w)/\binom{n}{w}$ is decreasing,

Progression

The double sphere

For $n = 2w - 1$, take $\mathcal{C}_0 = \mathcal{S}_n(w-1) \cup \mathcal{S}_n(w)$. Witnesses : support or co-support.

Proposition

$$\binom{2w}{w} \leqslant f(2w-1, w)$$

By extension : take $\mathcal{C} = \{cx; c \in \mathcal{C}_0, x \in \mathbb{F}_2^\ell\}$

Proposition

$$\forall w > n/2, \quad \binom{2(n-w+1)}{n-w+1} \leqslant f(n, w)$$

A construction for $n = 2w$

Codewords of $\mathcal{C}$ are

Type	Codeword	Witness
A	$111x$, with $x \in \mathcal{S}_{n-3}(w-2)$	$\{1,2\} \cup \mathrm{Supp}(x)$
B	$011x$, with $x \in \mathcal{S}_{n-3}(w-2)$	$\{1,3\} \cup \mathrm{Supp}(x)$
C	$010x$, with $x \in \mathcal{S}_{n-3}(w-1)$	$\{2\} \cup \mathrm{Supp}(x)$
D	$101x$, with $x \in \mathcal{S}_{n-3}(w-1)$	$\{3\} \cup \mathrm{Supp}(x)$
E	$100x$, with $x \in \mathcal{S}_{n-3}(w)$	$\mathrm{Supp}(x)$

Proposition

$$\forall w \geqslant 2, \quad \binom{2w}{w} + \binom{2w-2}{w-1} \leqslant f(2w, w)$$

Translates of classical codes

Let $\mathcal{C}_0 \subseteq \mathbb{F}_2^n$ a code with Hamming minimal distance $d \geqslant 2(n-w)+1$ and

$$\mathcal{C} = \{c_0 + x\,;\ c_0 \in \mathcal{C}_0,\ x \in \mathcal{S}_n(n-w)\}.$$

Witness of $c_0 + x \in \mathcal{C}$: complement of Supp$x$.

Proposition

$$\forall w > (n+1)/2, \quad \binom{n}{w} A_2\left(n, 2(n-w)+1\right) \leqslant f(n,w),$$

where $A_2(n,d)$ is the largest size of a length n code with minimal distance d.

Example : Let $r \geqslant 3$. With $\mathcal{C}_0$ the $[2^r-1, 2^r-r-1, 3]_2$ Hamming code, we get $(2^r-1)2^{2^r-r-1} \leqslant f(2^r-1, 2^r-2)$.
With $\mathcal{C}_0$ = extended Golay code, we get $8290304 \leqslant f(24,21)$.

Progression

$f(n, w)$ as an independance number

Let $\Gamma = (V, E)$ be the proximity graph with edges $V = \mathbb{F}_2^n \times \binom{[n]}{w}$ and vertices(x, W) et (x', W') if $x_{|W} = x'_{|W}$ or $x_{|W'} = x'_{|W'}$.

$$f(n, w) = \alpha(\Gamma) \quad \text{(independance number)}$$

A semidefinite program through Lovász ϑ number

$$\vartheta'(\Gamma) = \max_{X \in \mathbb{R}^{V \times V}} \langle J, X \rangle$$

$$\text{such that } \begin{cases} \langle I, X \rangle & = & 1 \\ X(v, v') & = & 0 \quad \text{if } (v, v') \in E \\ X & \geqslant & 0 \\ X & \succcurlyeq & 0 \end{cases}$$

where $\mathbb{R}$ is the real field, I the identity matrix, J the all-one matrix, $X \succcurlyeq 0$ means X is positive semidefinite.

Proposition

$$f(n, w) = \alpha(\Gamma) \leqslant \vartheta'(\Gamma)$$

Symmetry of the program

The graph Γ is invariant under the hyperoctaedral group $\mathfrak{H} = \mathbb{F}_2^n \rtimes \mathfrak{S}_n$ (translations and permutations). So we can consider only $\mathfrak{H}$-invariant matrices X in the semidefinite program.
Entries in the matrix X depend only on

$$\underline{\mathrm{d}} = (\iota, d_i, d_l, d_r, d_t) = \Big(|W \cap W'|, d_{W \cap W'}(x, x'),$$

$$d_{W \smallsetminus W \cap W'}(x, x'), d_{W' \smallsetminus W \cap W'}(x, x'), d_{[n] \smallsetminus W \cup W'}(x, x') \Big)$$

where d_A the Hamming distance on $A \subseteq [n]$.

Characterisation of positive semidefinite matrix

Theorem (Bochner)

There exists a basis of matrix valued functions $\underline{\mathrm{d}} \mapsto Z_k(\underline{\mathrm{d}})$ *called zonal functions such that* $X \succcurlyeq 0$ *is equivalent to*

$$\forall \underline{\mathrm{d}} \in \mathcal{D}, \quad X(\underline{\mathrm{d}}) = \sum_k \langle \Phi_k, Z_k(\underline{\mathrm{d}}) \rangle ,$$

where the $(\Phi_k)_k$ *are* $\succcurlyeq 0$ *matrix.*

"A semidefinite positive kernel has $\succcurlyeq 0$ Fourier coefficients and vice versa."

Theoretic expression of the zonal functions

Let $\mathbf{H}_k$ be a familly of representatives of the irreducible representations of $\mathfrak{H}$ and d_k their dimensions.
Let $\mathbb{C}^V = \bigoplus_k \bigoplus_{j=1}^{m_k} \mathbf{H}_{k,j}$ be a decomposition of $\mathbb{C}^V$ into irreducible subrepresentations with multiplicity denoted m_k.
Let $e_{k,j,\ell}$ be the copy of an orthonormal basis of $\mathbf{H}_k$ dans $\mathbf{H}_{k,j}$.

Then the zonal function Z_k is the $m_k \times m_k$-matrix-valued function defined over $V \times V$ by

$$\left(Z_k(v,v')\right)_{j_1,j_2} = \sum_{\ell=1}^{d_k} e_{k,j_1,\ell}(v)\overline{e_{k,j_2,\ell}(v')}.$$

Decomposition into irreducible's of $\mathbb{C}^V$ under $\mathfrak{H} = \mathbb{F}_2^n \rtimes \mathfrak{S}_n$

For $I \subseteq [n]$, we denote

$$\chi_I := x \in \mathbb{F}_2^n \mapsto (-1)^{\mathrm{wgt}(x_I)} \in \mathbb{C}.$$

We denote $\mathbf{S}^s_{[i]}$ the irreducible representation (Specht module) of $\mathfrak{S}_{[i]}$ associated with the partition $i = (i-s)+s$. We recall that $\mathbb{C}^{\binom{[i]}{j}} = \bigoplus_{j=0}^{i} \mathbf{S}^s_{[i],j}$. Then we get the irreducible representation

$$\mathbf{T}^j_{i,s,t} = \left(\chi_{[i]} \otimes \mathbf{S}^s_{[i],j} \otimes \mathbf{S}^t_{[i+1,n],w-j}\right) \uparrow^{\mathfrak{H}}_{\mathbb{F}_2^n \rtimes (\mathfrak{S}_{[i]} \times \mathfrak{S}_{[i+1,n]})}.$$

and the decomposition can be written as

$$\mathbb{C}^V = \bigoplus_{i=0}^{n} \bigoplus_{j=\max(0,w+i-n)}^{\min(w,i)} \bigoplus_{\substack{0 \leqslant s \leqslant \min(j,i-j),\\ 0 \leqslant t \leqslant \min(j,n-i-j)}} \mathbf{T}^j_{i,s,t}.$$

Computation of the zonal functions

We deduce

$$Z^{\mathbf{k}}_{j_1,j_2}\left((x,W),(x',W')\right)$$

$$= \sum_{\substack{I\in\binom{[n]}{w}\\ |W\cap I|=j_1,\\ |W'\cap I|=j_2}} (-1)^{\mathrm{wgt}(x_{|I}-x'_{|I})}\mathrm{Hahn}^{s}_{i,j_1,j_2}(|W\cap W'\cap I|)\mathrm{Hahn}^{t}_{\breve{i},\breve{j_1},\breve{j_2}}(|W\cap W'\cap I^c|)$$

where $\breve{i}=n-i$, $\breve{j_1}=w-j_1$, $\breve{j_2}=w-j_2$.

Computation of the zonal functions

- Zonal functions are naturally orthogonal as the subrepresentations are.
- We just need to focus on their dominant term. We expand the previous expression and compare with the expansion of the suggested monomials in the basis of the functions χ_i

$$\chi_k(x) = \begin{cases} 1 \text{ if } x_k = 1 \\ 0 \text{ if } x_k = 0 \end{cases}$$

and their product.

Zonal functions

In our case :

Proposition

The zonal functions $Z_{(i,s,t),j_1,j_2}$ can be computed by a Gram-Schmidt process on the monomials

$$\sum_{\substack{\alpha+\beta+\gamma+\delta=i,\\ \beta+\delta=j_1,\gamma+\delta=j_2}} \binom{\delta}{s} \frac{\iota^t \; {d_t}^\alpha \; {d_l}^\beta \; {d_r}^\gamma \; {d_i}^\delta}{\alpha!\;\beta!\;\gamma!\;\delta!}.$$

ordered by lex order on (i, t, s, j_1, j_2).

A new equivalent program

$$\vartheta'(\Gamma) = \max_{y \in \mathbb{R}^{|\mathcal{D}|}} \sum_{\underline{d} \in \mathcal{D}} y_{\underline{d}}$$

$$\text{such that} \begin{cases} y_{(w,0,0,0,0)} = 1 & \\ y_{\underline{d}} = 0 & \text{if } \underline{d} \in \mathcal{D}_o \\ y_{\underline{d}} \geqslant 0 & \text{for any } \underline{d} \in \mathcal{D} \\ \sum_{\underline{d}} y_{\underline{d}} Z_{i,s,t}(\underline{d}) \succcurlyeq 0 & \text{for any} (i,s,t) \end{cases}$$

Linear number of variables in n.

Numerical results (1)

n	$w=2$	$w=3$	$w=4$	$w=5$	$w=6$	$w=7$
3	6.00 6^b	8.00 8^b				
4	8.00 8^c	12.56 12^b	16.00 16^b			
5	10.56 10^a	20.00 20^b	26.15 25^e	32.00 32^b		
6	15.00 15^a	28.03 26^c	42.66 40^b	54.35 52^e	64.00 64^b	
7	21.00 21^a	39.31 35^a	70.00 70^b	90.30 80^b	112.00 112^d	128.00 128^b
8	28.00 28^a	56.65 56^a	102.15 90^c	150.61 140^b	189.27 160^b	226.86 224^b
9	36.00 36^a	84.00 84^a	149.05 126^a	252.00 252^b	321.31 280^b	393.34 320^b

Numerical results (2)

10	45.00 45^a	120.00 120^a	219.30 210^a	380.05 322^c	544.45 504^b	677.81 560^b
11	55.00 55^a	165.00 165^a	330.41 330^a	569.31 462^a	924.00 924^b	1166.08 1004^b
12	66.00 66^a	220.00 220^a	495.00 495^a	856.16 792^a	1422.87 1176^c	2000.21 1848^b
13	78.00 78^a	286.00 286^a	715.00 715^a	1304.65 1287^a	2184.91 1716^a	3432.00 3432^b
14	91.00 91^a	364.00 364^a	1001.00 1001^a	2002.00 2002^a	3349.38 3003^a	
15	105.00 105^a	455.00 455^a	1365.00 1365^a	3003.00 3003^a	5168.18 5005^a	
16	120 120^a	560.00 560^a	1820.00 1820^a	4368.00 4368^a	8024.58 8008^a	
17	136 136^a	680.00 680^a	2380.00 2380^a	6188.00 6188^a	12376 12376^a	

Results

1. For $w = 2$ and $n \geqslant 5$, $w = 3$ and $n \geqslant 8$, $w = 4$ and $n \geqslant 11$, $w = 5$ and $n \geqslant 14$, $w = 6$ and $n \geqslant 17$, we have
$$f(n, w) = \binom{n}{w}.$$
2. When $w = 2$, we have
$$f(2w, w) = \binom{2w}{w} + \binom{2w-2}{w-1}.$$
3. For $w \in \{2, \ldots, 7\}$, we have
$$f(2w-1, w) = \binom{2w}{w}.$$
4. We have
$$f(4, 3) = 12, \quad f(7, 6) = 112.$$

Summary and future work

We have

- constructed first examples of large witness code for small parameters n and w,
- disproved some previous guess about the maximal size,
- shown the maximality of our constructions in some cases.

We are still working on

- pushing the semidefinite programming technique to more general cases and understand where it works.

We need ideas

- where semidefinite programming doesn't work.

Thank you for your attention.

Questions.