Algebraic Construction of Good Collision Resistant Signal sets

Joint work by:

Marcus Greferath† and **Emanuele Viterbo**‡

† AT&T Shannon Labs – Florham Park – NJ – USA

‡ Dipartimento di Elettronica – Politecnico di Torino – Italy

Presentation outline

- Introduction
- The multiple access slotted collision channel
- Collision Resistant Modulation
- Algebraic construction
- Results
- Conclusions

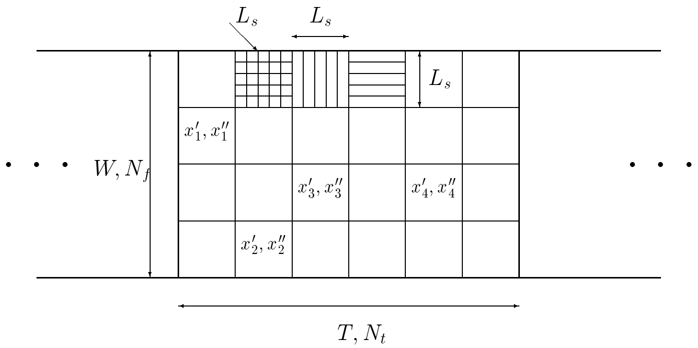
Introduction

- Multi-user, random access, time-frequency hopping, wireless network.
- Collisions occur among different users accessing the same channel slots, (e.g. as in a slotted ALOHA protocol).
- Signal-space code with D-dimensional signals. Each component is sent over a different channel slot and can be independently affected by a collision.
- CRMs have the property that even if $k < D$ slots collide the signal can still be correctly detected, in the absence of noise, from its $D - k$ un-collided components.

The multiple access slotted collision channel

- N_u number of active users
- $N_s = N_t \times N_f$ number of available slots where N_f is the number of carriers and N_t is the number of time slots per frame
- L_s number of real dimensions per slot
- $N_s L_s = 2WT$ where T is the time duration of a frame and W is the overall system bandwidth
- R_b [bits/frame] is the user transmission bit rate
- η [bits/dim] is the spectral efficiency of the modulation scheme
- $g = R_b/(\eta L_s)$ is the number slots per frame occupied by a user

The frame structure



$L_s = 2 \quad D = 4 \quad \mathbf{x}' = (x'_1, \ldots x'_4)^T \quad \mathbf{x}'' = (x''_1, \ldots x''_4)^T$

The multiple access slotted collision channel

- We model the transmission process of each user in each slot, as a Bernoulli process with parameter $p = g/N_s = R_b/(2WT\eta)$ representing the probability that one user occupies one slot.
- The probability of a collision in one slot is
$$P_c = 1 - (1-p)^{N_u - 1}$$
- In the limit case for $N_s, N_u \to \infty$ (i.e. infinite users population) the number of transmitting users in each slot becomes a Poisson distributed random variable with average $G = \lim_{N_s, N_u \to \infty} gN_u/N_s$ and
$$P_c = 1 - e^{-G}$$
- The parameter G corresponds to the so called *offered channel traffic*.

The Collision+Fading Vector Channel Model

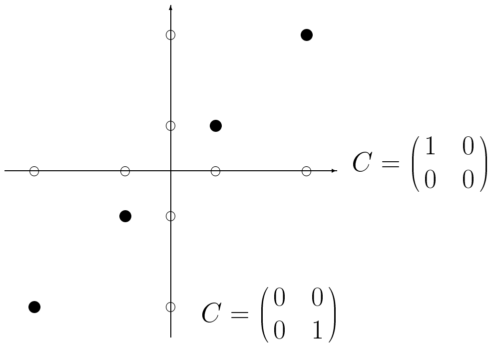
$$\boxed{\mathbf{y} = \mathrm{C}(\mathrm{G}\mathbf{x} + \mathbf{n})}$$

- $\mathbf{y} = (y_1, \ldots y_D)^T$ is a received vector
- $\mathbf{x} = (x_1, \ldots x_D)^T$ is a transmitted vector taken from the signal set (signal-space code) S of cardinality $|S|$
- $\mathbf{n} = (n_1, \ldots n_D)^T$ is additive white Gaussian noise with i.i.d. components $n_i = \mathcal{N}(0, N_0/2)$
- $G = diag(g_1, \ldots g_D)$ represents the channel fading coefficients
- $C = diag(c_1, \ldots c_D)$ represents the collision pattern and $c_i = 0$ or 1 are Bernoulli i.i.d. random variables with $P_c = P(c_i = 0)$.

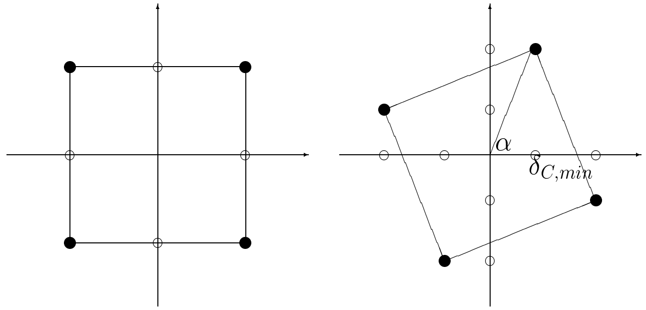
Collision Resistant Modulation

- The receiver has perfect channel state information (CSI) on both the collisions and the fading. ML detection is obtained for
$$\min_{\mathbf{x} \in S} d^2_C(\mathbf{x}, \mathbf{y}) \ = \ \min_{\mathbf{x} \in S} \sum_{i=1}^{D} c_i (y_i - g_i x_i)^2$$
- Let $S(C)$ be the projection of S on the subspace generated by the $D - k$ axes corresponding to the non zero c_i's
- A **Collision Resistant Modulation** (CRM) is a signal-space code S with the property that any projection on any coordinate subspace has the same number of distinct points as the original set, i.e., $|S(C)| = |S|$ for all non-zero collision patterns C.

Collision Resistant Modulation – Example 1



Collision Resistant Modulation – Example 2



Error Probability

- The symbol error probability is given by

$$P(e) = \sum_C P(C)P(e|C)$$

where C runs over all 2^D collision patterns,

$$P(C) = P_c^k(1 - P_c)^{D-k}$$

is the probability of a collision pattern C with k collisions and by using the Union bound

$$P(e|C) \leq \frac{1}{M} \sum_{\mathbf{x} \in S_C} \sum_{\mathbf{x} \neq \hat{\mathbf{x}}} P(\mathbf{x} \to \hat{\mathbf{x}})$$

where $P(\mathbf{x} \to \hat{\mathbf{x}})$ is the pairwise error probability averaged with respect to G.

Distance types

- On the pure AWGN channel without fading we consider the Squared Euclidean distance

$$d_E^2(\mathbf{s}, \mathbf{t}) := \|\mathbf{s} - \mathbf{t}\|_2^2 = \sum_{i=1}^{D} |s_i - t_i|^2$$

- On the independent Rayleigh fading channel (g_i are real independent Rayleigh distributed r.v.) we consider the Product distance.

$$d_P(\mathbf{s}, \mathbf{t}) := \prod_{i=1}^{D} |s_i - t_i|$$

- On the independent Rice fading channel (g_i are real independent Rice distributed r.v.) we consider the ℓ_1-distance

$$d_L(\mathbf{s}, \mathbf{t}) := \|\mathbf{s} - \mathbf{t}\|_1 = \sum_{i=1}^{D} |s_i - t_i|$$

The algebraic construction

- Let $\mathbb{Z}_M$ denote the ring of integers modulo M where $M = 2^m$, and write $\mathbb{Z}_M = \{-M/2+1, \dots M/2\}$.
- Consider linear codes of rank 1 over $\mathbb{Z}_M$, generated by $\mathbf{v} = (v_1, \dots v_D)$:
$$\mathcal{C} = \{\beta\mathbf{v} | \beta \in \mathbb{Z}_M\}$$
- As corresponding signal set S we take the code words identically embedded as real-valued vectors into the Euclidean space $\mathbb{R}^D$.
- For *collision resistance* all v_i must be units of $\mathbb{Z}_M$. In fact the i-th component βv_i of each codeword are all distinct as β runs over $\mathbb{Z}_M$. For $M = 2^m$ the unit group $U(\mathbb{Z}_M)$ is the set of odd numbers in $\mathbb{Z}_M$.

Signal sets in dimension $D = M/4 = 2^{m-2}$

Let $\mathbf{v} = (1, 3, \dots, M/2-1)$ then for the $[M/4, 1]$ code $\mathcal{C}$ generated by $\mathbf{v}$ the following holds:

1. the minimum Lee weight of $\mathcal{C}$ is $M^2/16$,
2. the minimum Euclidean weight of $\mathcal{C}$ is $M^3/64$
3. the minimum product weight of $\mathcal{C}$ is $(M/2-1)!!$

D	M	$d_{L,min}$	$d^2_{E,min}$	$d^{1/D}_{P,min}$
4	16	16	64	3.201
8	32	64	512	18.255
16	64	256	4096	759.473
32	128	1024	32768	$1.963 \cdot 10^6$
64	256	4096	262144	$2.524 \cdot 10^{13}$

Signal sets in dimension $D = m$

- To improve the spectral efficiency of the previous signal sets we should consider some punctured versions of the codes. The case $D = m$ corresponds to 1 bit/dim spectral efficiency.
- By exhaustive search through all $\mathbf{v} = (1, v_2, \dots v_D)$ and $v_i \in U(\mathbb{Z}_M)$ we found the following codes

D	M	$d_{L,min}$	$\mathbf{v}$
4	16	16	[1,3,5,7]
5	32	30	[1,3,5,11,15]
6	64	68	[1,3,5,17,23,31]
7	128	159	[1,5,17,25,27,57,63]

Signal sets in dimension $D = m$

D	M	$d^2_{E,min}$	$\mathbf{v}$
4	16	64	[1,3,5,7]
5	32	253	[1,3,5,7,15]
6	64	1222	[1,3,5,7,17,31]
7	128	5488	[1,3,5,23,33,49,63]

D	M	$d^{1/D}_{P,min}$	$\mathbf{v}$
4	16	3.201	[1,3,5,7]
5	32	4.638	[1,3,5,11,15]
6	64	8.363	[1,7,13,17,23,31]
7	128	15.554	[1,15,17,19,27,39,63]

An algebraic construction in dimension $D = m$

Consider the generating vectors $\mathbf{v} = (1, |\alpha|, |\alpha^2| \ldots |\alpha^{D-1}|)$, where α is selected among the elements of maximal order of $U(\mathbb{Z}_M)$. For $M = 2^m$ and $M \geq 16$ they are $(8k \pm 3) \pmod{M}$.

D	M	$d_{L,min}$	α_{opt}	$\mathbf{v}$
4	16	16	3,5	[1,3,7,5]
5	32	29	3,5,11,13	[1,3,9,5,15]
6	64	(60) 66	19,27	[1,19,23,11,17,3]
7	128	(107) 145	11,19,27,35	[1,11,7,51,49,27,41]
8	256	(256) 324	35,117	[1,35,55,123,47,109,25,107]
9	512	(489) 679	109,155	[1,109,105,181,239,61,7,251,223]
10	1024	(932) 1576	293,339	[1,293,167,221,241,43,311,13,287,123]

We conjecture the above construction produces comparatively good signal sets.

D	M	$d^2_{E,min}$	α_{opt}	$\mathbf{v}$
4	16	64	3,5	[1,3,7,5]
5	32	(237) 253	5,13	[1,5,7,3,15]
6	64	(942) 1118	11,29	[1,3,9,11,17,3]
7	128	(3023) 4444	3,43	[1,3,9,27,47,13,39]
8	256	(12392) 18600	5,51	[1,5,25,125,113,53,9,45]
9	512	(39657) 85897	45,91	[1,45,23,11,17,253,121,187,223]
10	1024	(159106) 354370	293,339	[1,293,167,221,241,43,311,13,287,123]

D	M	$d^{1/D}_{P,min}$	α_{opt}	$\mathbf{v}$
4	16	3.201	3,5	[1,3,7,5]
5	32	(4.237) 4.309	3,11	[1,3,9,5,15]
6	64	(6.289) 7.911	19,27	[1,19,23,11,17,3]
7	128	(8.287) 14.581	19,27	[1,19,23,53,17,61,7]
8	256	(14.987) 25.545	35,117	[1,35,55,123,47,109,25,107]
9	512	(22.383) 49.926	35,117	[1,35,201,133,47,109,231,107,161]
10	1024	(46.491) 95.459	251,461	[1,251,487,381,399,203,247,467,481,101]

Comparison with rotated hypercube

- We upper-bound the error probability by

$$P(e) \leq \sum_{k=0}^{4} \binom{D}{k} P_c^k (1 - P_c)^{D-k} P_{\max}(e|k)$$

  where $P_{\max}(e|k)$ is the largest error probability for given a collision pattern with k collisions.

- In the case of an AWGN channel we simply approximated $P_{\max}(e|k)$ with $\frac{1}{2}\mathrm{erfc}(d_{k,\min}/(2\sqrt{N_0}))$ where $d_{k,\min}$ is the smallest entry in the k-th row of following Tables.

Projection distances

- Squared Euclidean distances of all the projections

Roteted Hypercube						
k	C with k collisions					
0	86					
1	32.88	32.88	32.88	32.88		
2	12.59	9.08	4.41	4.41	9.08	12.59
3	0.06	0.06	0.06	0.06		

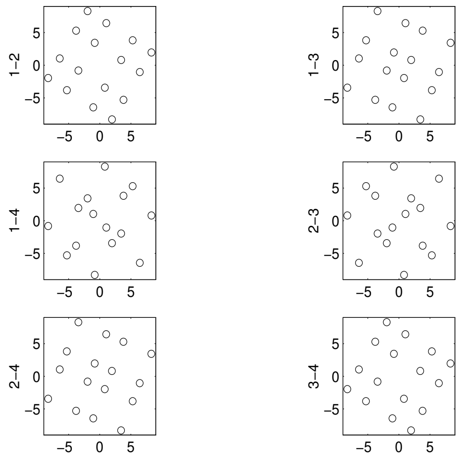
$\mathbb{Z}_{16}$ signal set						
k	C with k collisions					
0	64					
1	35	35	35	35		
2	10	10	8	8	10	10
3	1	1	1	1		

- Product distances of all the projections

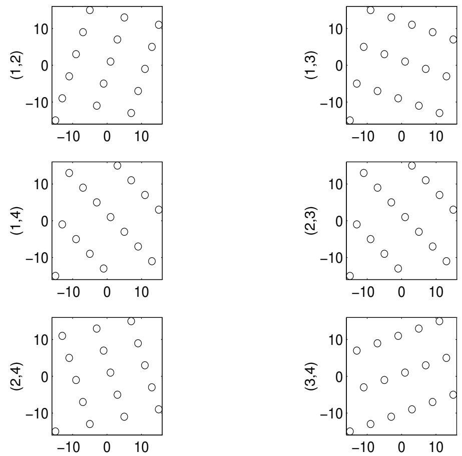
Roteted Hypercube						
k	C with k collisions					
0	184.9					
1	12.48	12.48	12.48	12.48		
2	2.33	1.98	2.21	2.21	1.98	2.33
3	0.24	0.24	0.24	0.24		

$\mathbb{Z}_{16}$ signal set						
k	C with k collisions					
0	105					
1	15	15	15	15		
2	3	3	4	4	3	3
3	1	1	1	1		

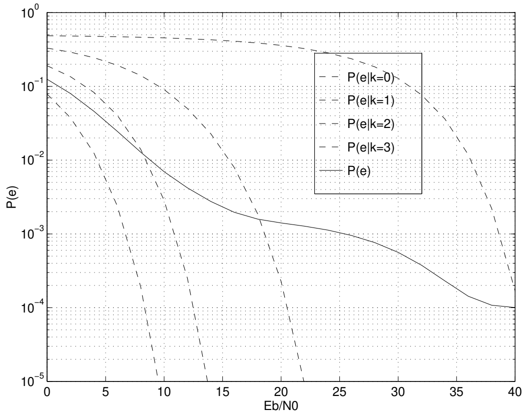
Rotated hypercube 2D projections



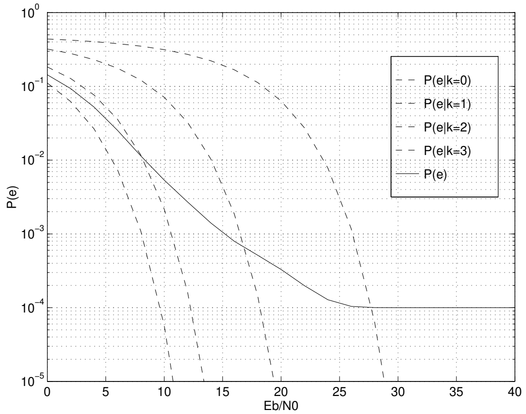
$\mathbb{Z}_{16}$ signal set 2D projections



Rotated D-hypercube signal set $P_c = 0.1$



Rotated $\mathbb{Z}_{16}$ signal set $P_c = 0.1$



Conclusions

- We have considered some algebraic constructions of collision resistant signal sets
- In some cases we are able to relate the code algebraic structure with the distance properties of the corresponding signal sets
- We believe that there may be other algebraic constructions which produce good signal sets
- We are currently investigating further this relation in order to prove our conjecture and design signal sets without having to perform an exhaustive search
- We expect to find at least some bounds for the signal set distances generated by certain particular families of codes.