

Group codes

An overview and new results

CMRR-UCSD

January 25, 2007

Fabio Fagnani

Dipartimento di Matematica, Politecnico di Torino, ITALY

Outline

- Historical remarks
- GU constellations
- Group codes: structural properties
- Group codes in turbo and low density schemes
- Performance of group codes: capacity, distance
- Conclusions

Historical remarks

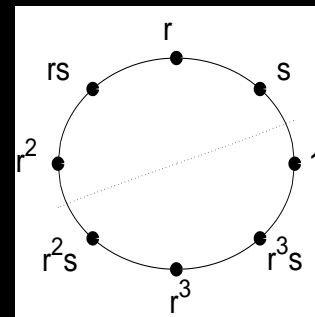
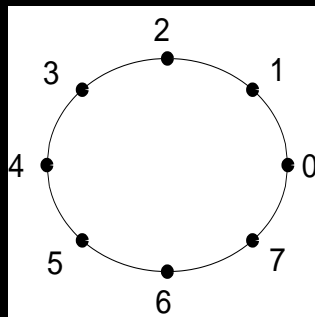
- D. Slepian, *Group codes for the Gaussian channel*, Bell Syst. Tech. J., 1968.
 - Slepian sets \leftrightarrow special finite GU constellations
- G. D. Forney, *Geometrically uniform codes*, IEEE Trans. Inf. Th., 1991.
 - A general theory: finite and infinite GU constellations and codes.
- Ingemarsson, Loeliger, Trott, Massey, Mittelholzer, Calderbank, Sloane, Benedetto, Biglieri, Caire, Elia, Garello, Montorsi, Divsalar, Zampieri, Johannesson, F.

GU Constellations

- $S \subseteq \mathbb{R}^q$ **GEOMETRICALLY UNIFORM** if

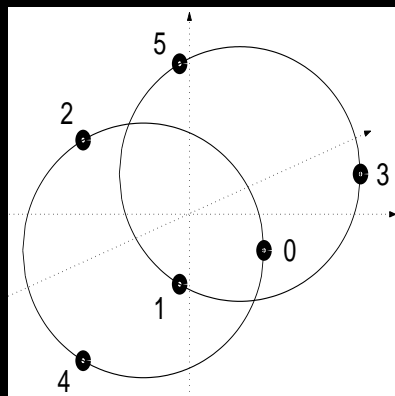
$$s_0, s_1 \in S \Rightarrow \exists g \in \text{Iso}(S) : gs_0 = s_1$$
- $G \leq \text{Iso}(S)$ **GENERATING GROUP** for S if

$$s_0, s_1 \in S \Rightarrow \exists! g \in G : gs_0 = s_1$$
- **LABELLING**: $\mu_0 : G \leftrightarrow S, \mu_0(g) = gs_0$;
- Ex: 8-PSK: $G = \mathbb{Z}_8$ OR $G = D_4$



Two 3-D examples

- 3-PSK \times 2-PAM: $G = \mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$

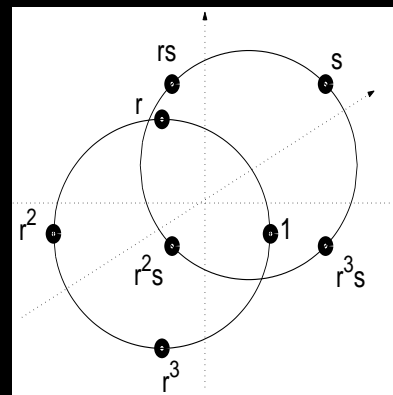
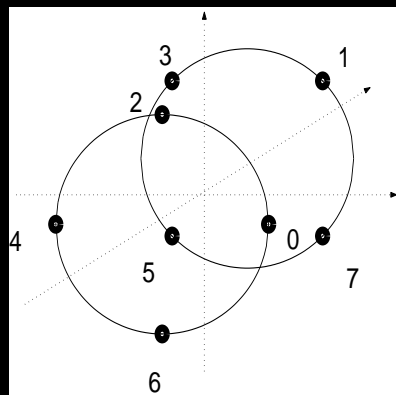


- $8h$ -PSK:

$$G = \mathbb{Z}_8$$

OR

$$G = D_4$$



Properties of GU constellations

$S \subseteq \mathbb{R}^q$ GU.

- Set of distances $\{\|s - s_0\| \mid s \in S\}$ **independent** of $s_0 \in S$.
- **Congruent** Voronoi regions.

AWGN channel (S -AWGN)

- input in S
- output unquantized or quantized
- ML decoded
- **UNIFORM ERROR PROPERTY (UEP):**

$$P_w(e) = P_w(e|s_0)$$

G -codes

A way to construct GU constellations of large length:

- Fix $S \subseteq \mathbb{R}^q$ GU
- Fix G be a generating group for S
- Fix $\mu : G \rightarrow S$ labelling.
- Choose $\mathcal{X} \subseteq G^N$ a subgroup.

$\mu : \mathcal{X} \mapsto \mathbb{R}^{qN}$ and the image is a GU constellation.

\mathcal{X} is called a G -code.

G -codes: structure properties

G -codes inherit many properties of linear codes:

G -codes: structure properties

G -codes inherit many properties of linear codes:

(Forney-Trott IT-1993, Loeliger-Mittelholzer IT-1996)

- G -codes admit **minimal trellis representations with group structure**
- G -codes admit **minimal feedbackfree encoders not in general homomorphic**
- theory extends (under mild technical conditions) to infinite length codes (convolutional codes)

G -codes: structure properties

G -codes inherit many properties of linear codes:

(Forney-Trott IT-1993, Loeliger-Mittelholzer IT-1996)

- G -codes admit **minimal trellis representations with group structure**
- G -codes admit **minimal feedbackfree encoders not in general homomorphic**
- theory extends (under mild technical conditions) to infinite length codes (convolutional codes)

(Zampieri-F. IT-1999)

- G -codes admit **minimal feedbackfree syndrome formers not in general homomorphic**

Techniques: behavioral systems theory (Willems)

Abelian G -codes

$G = \mathbb{Z}_m$, cyclic group. $A \in \mathbb{Z}_m^{K \times N}$ matrix.

$\ker A \subseteq \mathbb{Z}_m^K$, $\text{Im} A \subseteq \mathbb{Z}_m^N$ are \mathbb{Z}_m -codes.

Additional structure: \mathbb{Z}_m -codes inherit a **module** structure over \mathbb{Z}_m .

Generating matrices and syndromes available as in the field case.

More general homomorphisms $\phi : \mathbb{Z}_{m_1}^{K_1} \oplus \dots \oplus \mathbb{Z}_{m_r}^{K_r} \rightarrow \mathbb{Z}_m^N$

Ex: $\phi : \mathbb{Z}_8^{K_1} \oplus \mathbb{Z}_4^{K_2} \oplus \mathbb{Z}_2^{K_3} \rightarrow \mathbb{Z}_8^N$

Convolutional codes I

$\mathbb{Z}_m((D))$ ring of Laurent series,

$\mathbb{Z}_m(D)$ rational functions: $\frac{a_0 + \dots + a_k D^k}{b_0 + \dots + b_h D^h}$, b_h invertible

$A(D) \in \mathbb{Z}_m(D)^{K \times N}$ homom. conv. encoder.

$\ker A(D) \subseteq \mathbb{Z}_m((D))^K$, $\text{Im} A(D) \subseteq \mathbb{Z}_m^N((D))$

convolutional \mathbb{Z}_m -codes.

Convolutional codes I

$\mathbb{Z}_m((D))$ ring of Laurent series,

$\mathbb{Z}_m(D)$ rational functions: $\frac{a_0 + \dots + a_k D^k}{b_0 + \dots + b_h D^h}$, b_h invertible

$A(D) \in \mathbb{Z}_m(D)^{K \times N}$ homom. conv. encoder.

$\ker A(D) \subseteq \mathbb{Z}_m((D))^K$, $\text{Im} A(D) \subseteq \mathbb{Z}_m^N((D))$

convolutional \mathbb{Z}_m -codes.

Problems:

- A convolutional code may not admit minimal homomorphic convolutional encoders.
- A convolutional code may admit minimal but no systematic homomorphic convolutional encoders.

Algebraic structure creates obstacles!

Convolutional codes II

Algebraic conditions for the existence of minimal convolutional encoder: $\mathcal{X} \subseteq \mathbb{Z}_m^N((D))$.

$$\mathcal{X}_+ = \mathcal{X} \cap \mathbb{Z}_m^N[[D]], \quad \mathcal{X}_{++} = \mathcal{X} \cap D\mathbb{Z}_m^N[[D]],$$

$$\mathcal{X}_- = \mathcal{X} \cap D^{-1}\mathbb{Z}_m^N[D^{-1}].$$

$U(\mathcal{X}) = \mathcal{X}_+/\mathcal{X}_{++}$ input group; $Z(\mathcal{X}) = \mathcal{X}/(\mathcal{X}_- \oplus \mathcal{X}_+)$ state group.

$$n \in \mathbb{Z}, \quad \mathcal{X}_{(n)} = \{x \in \mathcal{X} \mid nx = 0\}$$

Theorem: (F.-Zampieri LAA-2004) The following are equivalent:

- \mathcal{X} admits a minimal hom. conv. encoder.
- $U(\mathcal{X}_{(n)}) = U(\mathcal{X})_{(n)}, Z(\mathcal{X}_{(n)}) = Z(\mathcal{X})_{(n)}, \forall n$.

\mathbb{Z}_8 : only need to check for $n = 2, 4$.

High performance schemes I

Group codes in turbo schemes:

- Maintain UEP.
- Optimize the constituent encoders for the chosen GU constellation.

1. R. Garello, G. Montorsi, S. Benedetto, D. Divsalar and F. Pollara, **Labelings and encoders with the uniform bit error property with applications to serially concatenated trellis codes**, *IEEE IT-48*, 2002.

2. F.F., B. Scanavino, R. Garello, S. Zampieri, **Some results on combined parallel concatenated schemes with trellis coded modulation**, ISIT 2002.

3. F.F., F. Garin, **Analysis of serial concatenation schemes for non-binary modulations**, ISIT 2005.

High performance schemes II

Group codes in low density schemes:

$$A \in \mathbb{Z}_m^{K \times N}$$

- c non-zero elements in each row,
- d non-zero elements in each column,
- non-zero elements chosen according to some distribution.

$$\mathcal{X} = \ker A.$$

1. A. Bennatan, D. Burshetein , **On The Application of LDPC Codes to Arbitrary Discrete Memoryless Channels**, *IEEE IT-50*, 2004.
2. D. Sridhara, T.E. Fuja, **LDPC Codes Over Rings for PSK Modulation**, *IEEE IT-51*, 2005.
3. G. Como, F.F., **Ensembles of Codes over Abelian Groups**, ISIT 2005.

Performance of group codes I

QUESTIONS: (Loeliger IT-1991)

- Given a group G , what type of GU constellations S have G as a generating group?

Assume that S has G as generating group.

- Do G -codes **achieve the capacity** of the $S - AWGN$ channel?
- What about **error exponents** and **minimum Euclidean distances**?

Performance of group codes II

Theorem: (Ingemarsson-Loeliger) Let $S \subseteq \mathbb{R}^q$ be a GU constellation admitting an Abelian generating group. Then there exists numbers $M_1, \dots, M_r \geq 3$ and q such that $2r + s = q$ and $S = M_1 - PSK \times \dots \times M_r - PSK \times (2 - PAM)^s$ (w.r. to a suitable orthonormal basis and with possibly different energies on the various components).

Corollary

$$\text{Cap}(S - \text{AWGN}) \leq \lim_{M \rightarrow +\infty} \text{Cap}(M - \text{PSK} - \text{AWGN})$$

Increase capacity \rightarrow Non-Abelian groups!

Performance of group codes III

Loeliger's conjecture: G generating group for S .
Then, G -codes achieve the capacity of the
 $S - AWGN$ channel.

Performance of group codes III

Loeliger's conjecture: G generating group for S .
Then, G -codes achieve the capacity of the
 $S - AWGN$ channel.

- $S = 2\text{-PAM}$, $G = \mathbb{Z}_2$, **YES!** classical result
(averaging technique+Gallager bound)

Performance of group codes III

Loeliger's conjecture: G generating group for S .
Then, G -codes achieve the capacity of the
 $S - AWGN$ channel.

- $S = 2$ -PAM, $G = \mathbb{Z}_2$, **YES!** classical result
(averaging technique+Gallager bound)
- $S = p$ -PSK, $G = \mathbb{Z}_p$ (p prime), **YES!**
(trivial extension)

Performance of group codes III

Loeliger's conjecture: G generating group for S .
Then, G -codes achieve the capacity of the
 $S - AWGN$ channel.

- $S = 2$ -PAM, $G = \mathbb{Z}_2$, **YES!** classical result
(averaging technique+Gallager bound)
- $S = p$ -PSK, $G = \mathbb{Z}_p$ (p prime), **YES!**
(trivial extension)
- $S = p^r$ -PSK, $G = \mathbb{Z}_{p^r}$ **YES!**
(G. Como, bach. thesis 2004)

Performance of group codes III

Loeliger's conjecture: G generating group for S .
Then, G -codes achieve the capacity of the
 $S - AWGN$ channel.

- $S = 2$ -PAM, $G = \mathbb{Z}_2$, **YES!** classical result
(averaging technique+Gallager bound)
- $S = p$ -PSK, $G = \mathbb{Z}_p$ (p prime), **YES!**
(trivial extension)
- $S = p^r$ -PSK, $G = \mathbb{Z}_{p^r}$ **YES!**
(G. Como, bach. thesis 2004)
- S generic, $G = \mathbb{Z}_M$ **IT DEPENDS.....**

Performance of group codes III

Loeliger's conjecture: G generating group for S .
Then, G -codes achieve the capacity of the
 $S - AWGN$ channel.

- $S = 2$ -PAM, $G = \mathbb{Z}_2$, **YES!** classical result
(averaging technique+Gallager bound)
- $S = p$ -PSK, $G = \mathbb{Z}_p$ (p prime), **YES!**
(trivial extension)
- $S = p^r$ -PSK, $G = \mathbb{Z}_{p^r}$ **YES!**
(G. Como, bach. thesis 2004)
- S generic, $G = \mathbb{Z}_M$ **IT DEPENDS.....**
- S generic, G non-Abelian **NO IDEA.....**

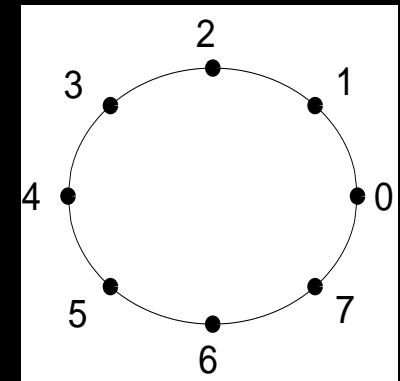
\mathbb{Z}_8 -codes for 8-PSK I

Notation: C_M capacity (bits/ch use) of (M -PSK)-AWGN.

- \mathbb{Z}_8 -code: $\mathcal{X} \leq \mathbb{Z}_8^N$; $\mathcal{X} \simeq \mathbb{Z}_8^{N_3} \oplus 2\mathbb{Z}_8^{N_2} \oplus 4\mathbb{Z}_8^{N_1}$

$$\text{rate: } R_8 = \frac{N_1 + 2N_2 + 3N_3}{N}$$

$$\text{Rel. transm.} \Rightarrow R_8 \leq C_8$$



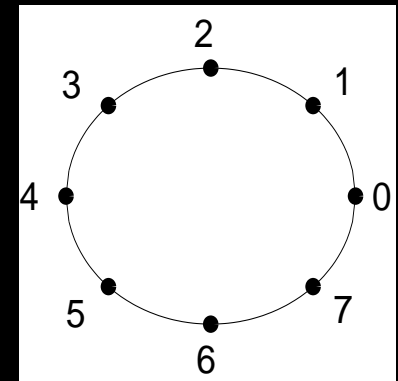
\mathbb{Z}_8 -codes for 8-PSK I

Notation: C_M capacity (bits/ch use) of (M -PSK)-AWGN.

- \mathbb{Z}_8 -code: $\mathcal{X} \subseteq \mathbb{Z}_8^N$; $\mathcal{X} \simeq \mathbb{Z}_8^{N_3} \oplus 2\mathbb{Z}_8^{N_2} \oplus 4\mathbb{Z}_8^{N_1}$

$$\text{rate: } R_8 = \frac{N_1 + 2N_2 + 3N_3}{N}$$

$$\text{Rel. transm.} \Rightarrow R_8 \leq C_8$$

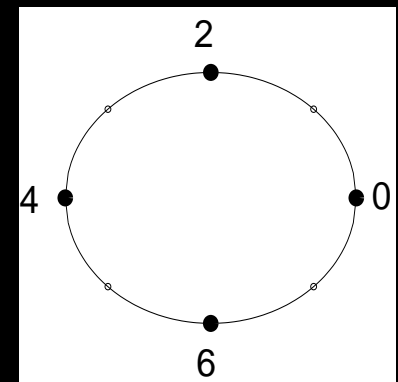


- subcode $\mathcal{X}_{(4)} := \mathcal{X} \cap 2\mathbb{Z}_8^N$;

$$\mathcal{X}_{(4)} \simeq 2\mathbb{Z}_8^{N_2 + N_3} \oplus 4\mathbb{Z}_8^{N_1}$$

$$\text{rate: } R_4 = \frac{N_1 + 2N_2 + 2N_3}{N} \geq \frac{2}{3}R_8$$

$$\mathcal{X}_{(4)} \subseteq 2\mathbb{Z}_8^N \text{ only sees 4-PSK:}$$



$$\frac{2}{3}R_8 \leq R_4 \leq C_4 !!$$

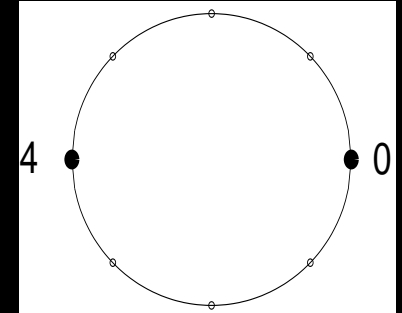
\mathbb{Z}_8 -codes for 8-PSK II

- subcode $\mathcal{X}_{(2)} := \mathcal{X} \cap 4\mathbb{Z}_8^N$; $\mathcal{X}_{(2)} \simeq 4\mathbb{Z}_8^{N_1+N_2+N_3}$

$$\text{rate: } R_2 = \frac{N_1+N_2+N_3}{N} \geq \frac{1}{3}R_8$$

$\mathcal{X}_{(2)} \subseteq 4\mathbb{Z}_8^N$ only sees **2-PSK**:

$$\frac{1}{3}R_8 \leq R_2 \leq C_2 \quad !!$$



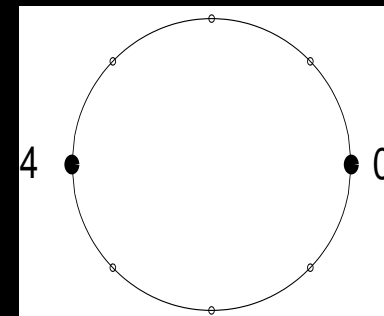
\mathbb{Z}_8 -codes for 8-PSK II

- subcode $\mathcal{X}_{(2)} := \mathcal{X} \cap 4\mathbb{Z}_8^N$; $\mathcal{X}_{(2)} \simeq 4\mathbb{Z}_8^{N_1+N_2+N_3}$

rate: $R_2 = \frac{N_1+N_2+N_3}{N} \geq \frac{1}{3}R_8$

$\mathcal{X}_{(2)} \subseteq 4\mathbb{Z}_8^N$ only sees **2-PSK**:

$$\frac{1}{3}R_8 \leq R_2 \leq C_2 \quad !!$$



- **Necessary** condition for reliable transmission with \mathbb{Z}_8 -codes:

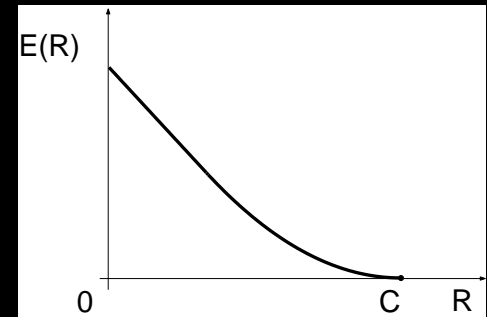
$$R_8 < \min \left\{ C_8, \frac{3}{2}C_4, 3C_2 \right\} =: C_{\mathbb{Z}_8}$$

$C_{\mathbb{Z}_8}$: \mathbb{Z}_8 -capacity of (8-PSK)-AWGN

Shannon coding theorem.

General memoryless channel with inputs in G :

- The average error exponent $E(R)$



- $K = \left\lceil N \frac{R}{\log |G|} \right\rceil$; $\Phi \sim Unif(\{\phi : G^K \rightarrow G^N\})$

$$\overline{P_w(e|\Phi)} \leq \exp(-NE(R));$$

- $R > C \Rightarrow P_w(e) \geq A_R > 0$;

Coding Theorem for \mathbb{Z}_8 -codes

\mathbb{Z}_8 -parity check ensemble:

$$\Phi_8 \sim \text{Unif}(\mathbb{Z}_8^{L \times N}), \quad \mathcal{X} = \ker \Phi_8, \quad R = 3 \frac{N-L}{N};$$

Theorem:

$$\overline{P(e)} \leq 2^{-NE_8(R)} + 2^{-NE_4(\frac{2}{3}R)} + 2^{-NE_2(\frac{1}{3}R)}$$

$E_l(R) = l$ -PSK random coding exponent

Coding Theorem for \mathbb{Z}_8 -codes

\mathbb{Z}_8 -parity check ensemble:

$$\Phi_8 \sim \text{Unif}(\mathbb{Z}_8^{L \times N}), \quad \mathcal{X} = \ker \Phi_8, \quad R = 3 \frac{N-L}{N};$$

Theorem:

$$\overline{P(e)} \leq 2^{-NE_8(R)} + 2^{-NE_4(\frac{2}{3}R)} + 2^{-NE_2(\frac{1}{3}R)}$$

$E_l(R) = l$ -PSK random coding exponent

Corollary:

$$R < C_{\mathbb{Z}_8} = \min\{C_8, \frac{3}{2}C_4, 3C_2\} \Rightarrow \overline{P(e)} \rightarrow 0$$

$\implies C_{\mathbb{Z}_8}$ is the capacity of \mathbb{Z}_8 -codes !!

Sketch of proof

- UEP \Rightarrow we suppose $\phi_8 \mathbf{0} = \mathbf{0}$ was transmitted
- ML error event $e = \{\mathbf{0} \rightarrow \mathbf{u} \neq \mathbf{0}\} = e_8 \cup e_4 \cup e_2$
 - $e_2 = \{\mathbf{0} \rightarrow \mathbf{u} \neq \mathbf{0} \mid 4 \mid \mathbf{u}\}$
 - $e_4 = \{\mathbf{0} \rightarrow \mathbf{u} \neq \mathbf{0} \mid 2 \mid \mathbf{u}, 4 \nmid \mathbf{u}\}$
 - e all the rest.
- $P_w(e|\Phi, \mathbf{0}) \leq P_w(e_8|\mathbf{0}) + P_w(e_4|\mathbf{0}) + P_w(e_2|\mathbf{0})$
- Gallager bound (Shulman-Feder) to each $P(e_i)$
- standard averaging for symmetric channels

Exact same proof for any S which has \mathbb{Z}_8 as generating group!

The general case

S with generating group \mathbb{Z}_{p^r} .

$$C_{\mathbb{Z}_{p^r}} := \min_{1 \leq s \leq r} \frac{r}{s} C_{p^s} \quad (C_{p^s} \text{ Shannon capacity of } p^{r-s} \mathbb{Z}_{p^r} \text{ subchannel})$$

Theorem:

- $R > C_{\mathbb{Z}_{p^r}}, \mathcal{X} \subseteq \mathbb{Z}_{p^r}^N \implies P(e) \geq A_R > 0$

- $\Phi \sim \text{Unif}(\mathbb{Z}_{p^r}^{N \times L}), R = \frac{N-L}{N} \log m$

$$R < C_{\mathbb{Z}_{p^r}} \implies \overline{P(e)} \leq \sum_{1 \leq s \leq r} 2^{-NE_{p^s}(\frac{s}{r}R)} \rightarrow 0$$

Generalizable to arbitrary finite Abelian group G : G -capacity.

G-capacity vs. Shannon capacity I

Theorem: For the p^r -PSK constellation, we have that

$$C_{\mathbb{Z}_{p^r}} = C_{p^r}$$

Proof (sketch):

- Recall $C_{\mathbb{Z}_{p^r}} = \min_{1 \leq s \leq r} \frac{r}{s} C_{p^s}$
- $(q+1)C_{p^q} \geq qC_{p^{q+1}}$
 - geometry of the PSK constellation
 - entropy inequalities
- $rC_p \leq \frac{r}{2}C_{p^2} \leq \dots \leq C_{p^r} = C.$

G -capacity vs. Shannon capacity I

Theorem: For the p^r -PSK constellation, we have that

$$C_{\mathbb{Z}_{p^r}} = C_{p^r}$$

Proof (sketch):

- Recall $C_{\mathbb{Z}_{p^r}} = \min_{1 \leq s \leq r} \frac{r}{s} C_{p^s}$
- $(q+1)C_{p^q} \geq qC_{p^{q+1}}$
 - geometry of the PSK constellation
 - entropy inequalities
- $rC_p \leq \frac{r}{2}C_{p^2} \leq \dots \leq C_{p^r} = C.$

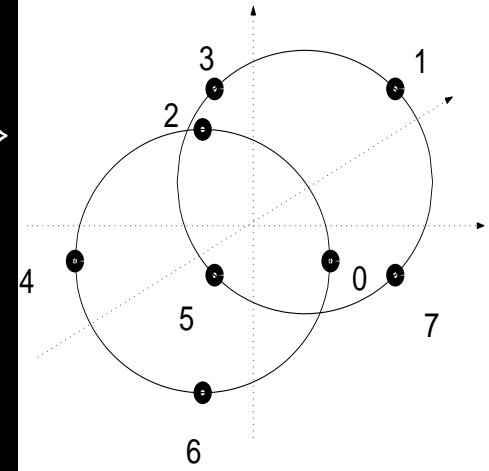
Corollary: \mathbb{Z}_{p^r} -codes **ACHIEVE** Shannon capacity of $(p^r$ -PSK)-AWGN

G -capacity vs. Shannon capacity II

$$K_8^\beta := \left\{ \left(\sqrt{\frac{1}{1+\beta^2}} e^{i\frac{2\pi}{8}k}, \sqrt{\frac{\beta^2}{1+\beta^2}} (-1)^k \right), k \in \mathbb{Z}_8 \right\}$$

$$\beta \rightarrow 0 \Rightarrow K_8^\beta \rightarrow 8\text{-PSK}$$

$$\beta \rightarrow +\infty \Rightarrow K_8^\beta \rightarrow 2\text{-PAM}$$



- for small β : $C_{\mathbb{Z}_8} = C_8$.
- for large β : $C_{\mathbb{Z}_8} < C_8$:

\mathbb{Z}_8 -codes cannot achieve Shannon capacity

What about D_4 -CODES??

Minimum Euclidean distances I

S GU const., G gen. group, $\mu_0 : G \leftrightarrow S$ labelling.

Square distance profile: $d(g) = \|\mu_0(g) - \mu_0(\mathbb{1}_G)\|^2$.

$\theta \in \mathcal{P}(G)$ distribution. $\langle d, \theta \rangle = \sum_g d(g)\theta(g)$

$\mathbf{x} \in G^N$, $\theta(\mathbf{x}) \in \mathcal{P}(G)$ **type** of \mathbf{x} .

Rel. Min. Dist.: $(\|\mu_0(\mathbf{x}) - \mu_0(\mathbf{y})\|^2 = N \langle d, \theta(\mathbf{xy}^{-1}) \rangle)$

$\mathcal{X} \subseteq G^N$, $\delta(\mathcal{X}) := \min\{\langle d, \theta(\mathbf{xy}^{-1}) \rangle \mid \mathbf{x} \neq \mathbf{y} \in \mathcal{X}\}$.

GV-bound:

$\delta^{GV}(R) := \inf \{ \langle \theta, d \rangle \mid \theta \in \mathcal{P}(G) : H(\theta) \geq R \log |G| \}$

Theorem: (Blahut IT-77)

$\sup \{ \delta(\mathcal{X}) \mid \mathcal{X} \text{ code over } G, R(\mathcal{X}) \leq R \} \geq \delta^{GV}(R)$

Minimum Euclidean dist. II

$\mathcal{X} \leq G^N$ group code.

$$\delta(\mathcal{X}) := \min\{\langle d, \theta(\mathbf{x}) \rangle \mid \mathbf{x} \in \mathcal{X} \setminus \{\mathbb{1}_G\}\}.$$

QUESTION:

$$\sup \{ \delta(\mathcal{X}) \mid \mathcal{X} \text{ } G\text{-code}, R(\mathcal{X}) \leq R \} \geq \delta^{GV}(R)$$

Minimum Euclidean dist. II

$\mathcal{X} \leq G^N$ group code.

$$\delta(\mathcal{X}) := \min\{\langle d, \theta(\mathbf{x}) \rangle \mid \mathbf{x} \in \mathcal{X} \setminus \{\mathbb{1}_G\}\}.$$

QUESTION:

$$\sup \{ \delta(\mathcal{X}) \mid \mathcal{X} \text{ } G\text{-code}, R(\mathcal{X}) \leq R \} \geq \delta^{GV}(R)$$

- Classical case $G = \mathbb{Z}_2$: **YES!** (with probability one!)

Minimum Euclidean dist. II

$\mathcal{X} \leq G^N$ group code.

$$\delta(\mathcal{X}) := \min\{\langle d, \theta(\mathbf{x}) \rangle \mid \mathbf{x} \in \mathcal{X} \setminus \{\mathbf{1}_G\}\}.$$

QUESTION:

$$\sup \{ \delta(\mathcal{X}) \mid \mathcal{X} \text{ } G\text{-code}, R(\mathcal{X}) \leq R \} \geq \delta^{GV}(R)$$

- Classical case $G = \mathbb{Z}_2$: **YES!** (with probability one!)
- $G = \mathbb{Z}_8$, $S = 8$ -PSK, **YES** (with probability one!)
(Como-F. ISIT-2007 submitted)

Minimum Euclidean dist. II

$\mathcal{X} \leq G^N$ group code.

$$\delta(\mathcal{X}) := \min\{\langle d, \theta(\mathbf{x}) \rangle \mid \mathbf{x} \in \mathcal{X} \setminus \{\mathbf{1}_G\}\}.$$

QUESTION:

$$\sup \{ \delta(\mathcal{X}) \mid \mathcal{X} \text{ } G\text{-code}, R(\mathcal{X}) \leq R \} \geq \delta^{GV}(R)$$

- Classical case $G = \mathbb{Z}_2$: **YES!** (with probability one!)
- $G = \mathbb{Z}_8$, $S = 8$ -PSK, **YES** (with probability one!)
(Como-F. ISIT-2007 submitted)
- $G = \mathbb{Z}_{p^r}$, $S = p^r$ -PSK, **YES (conjectured...)**

Conclusions

Group codes have been introduced in 1968 and widely studied during the 90's. By now they form a fairly well established and elegant theory. Recent contributions also show potential applications in high performance codes. However, many basic questions are still open:

- **When \mathbb{Z}_{p^r} -codes achieve capacity:**
 - Is $\min E_{p^s} \left(\frac{s}{r} R \right)$ the correct average error exponent?
 - Concentration?
 - Comparison with linear binary codes (error exponents, distances).
- **When \mathbb{Z}_{p^r} -codes do not achieve capacity:**
 - Other group codes?