Bounds for codes on pentagon (and other cycles)

Marco Dalai [1,3] Yury Polyanskiy [2,3]

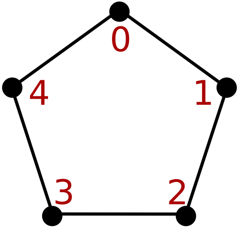
[1]Dept. Inform. Engineering
U. of Brescia, Italy
marco.dalai@unibs.it

[2]Department of EECS
MIT
yp@mit.edu

[3]**Thanks:** Simons Institute @ UC Berkeley (!)

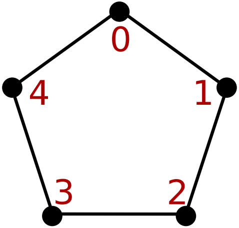
Allerton Conference, Oct 1, 2015

Zero-error typing



- Let $c_1, \ldots, c_n \in \{0,1,2,3,4\}^n$ – account number.
- Entering c_j can mistype $c_j \pm 1 \mod 5$.
- Goal: Find many non-confusable numbers of length n

Zero-error typing

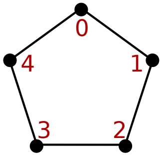


- Let $c_1, \ldots, c_n \in \{0,1,2,3,4\}^n$ – account number.
- Entering c_j can mistype $c_j \pm 1 \mod 5$.
- Goal: Find many non-confusable numbers of length n
- Shannon-Lovász:

$$\text{optimum} = (\sqrt{5})^n(1 + O(1)) \qquad \text{Rate} = \frac{1}{2}\log 5\,.$$

- Today: What if typist can make at most δn mistakes?

Main results



Theorem

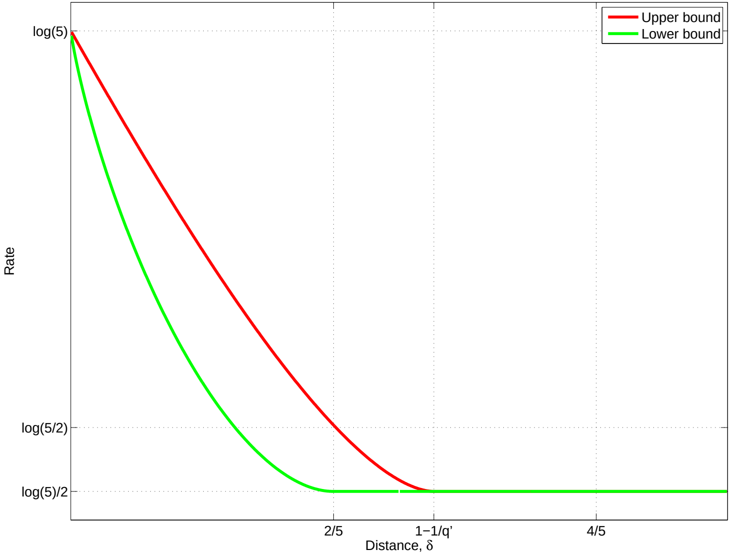
Maximal rate $R^*(\delta)$ satisfies:

$$\frac{1}{2}\log 5 + \frac{1}{2}R_{GV}(2\delta; 5) \le R^*(\delta) \le \frac{1}{2}\log 5 + R_{LP}(\delta; \sqrt{5}) \,.$$

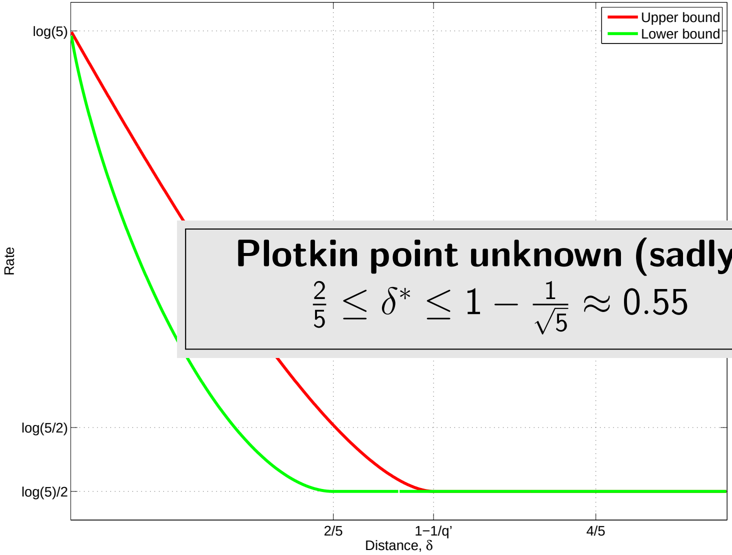
where $R_{GV}(\cdot; q)$ – q-ary Gilbert-Varshamov bound
and $R_{LP}(\cdot; q)$ – q-ary Linear-Programming bound.

- Imaginary $\sqrt{5}$-ary Hamming space appears (!).
- $\cdots$ $R^* = \frac{1}{2}\log 5$ for $\delta > 1 - \frac{1}{\sqrt{5}}$
- $\cdots$ $R^* > \frac{1}{2}\log 5$ for $\delta < \frac{2}{5}$.

Main results: plot



Main results: plot



Plotkin point unknown (sadly):

$$\frac{2}{5} \le \delta^* \le 1 - \frac{1}{\sqrt{5}} \approx 0.55$$

Background: Pentagon Combinatorics

Shannon capacity of a graph

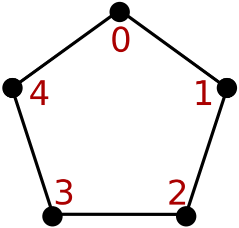
Definition

Strong power G^n of graph G is:

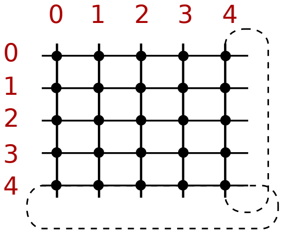
- Vertices: $V(G^n) \triangleq V(G) \times \cdots \times V(G)$
- Edges: $\mathbf{g} \sim \mathbf{g}'$ if all entries are adjacent or equal, i.e.

$$(g_1, \ldots, g_n) \sim (g_1', \ldots, g_n') \iff \forall i : g_i \sim g_i' \text{ or } g_i = g_i'$$

$\boxed{n = 1}$



$\boxed{n = 2}$



Shannon capacity of a graph

Definition (Shannon capacity $C(G)$)

$$C(G) \triangleq \lim_{n\to\infty} \frac{1}{n} \log \alpha(G^n)\,.$$

where $\alpha(\cdot)$ = size of max. independent set (subgraph w/o edges)

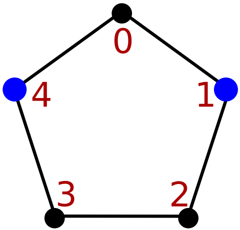
Shannon capacity of a graph

Definition (Shannon capacity $C(G)$)

$$C(G) \triangleq \lim_{n\to\infty} \frac{1}{n} \log \alpha(G^n)\,.$$

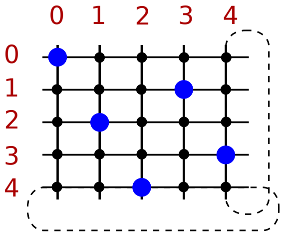
where $\alpha(\cdot)$ = size of max. independent set (subgraph w/o edges)

$\boxed{n=1}$



$R = 1$

$\boxed{n=2}$



$R = \frac{1}{2}\log 5$ (bit/ch.use)

Lovász' bound

- Associate to every $v \in G$ unit vector $e_v \in \mathbb{R}^d$ s.t.

$$v \not\sim v' \implies e_v \perp e_{v'}$$

- S – independent set $\iff$ $\{e_v, v \in S\}$ orthonormal subset
- $\implies S$ cannot be too big, since $\forall b \in \mathbb{R}^d$

$$\|b\|^2 \geq \sum_{v \in S} (e_v, b)^2 \geq \frac{|S|}{\theta},$$

where

$$\theta = \left(\min_{v \in V(G)} (e_v, b)^2 \right)^{-1}$$

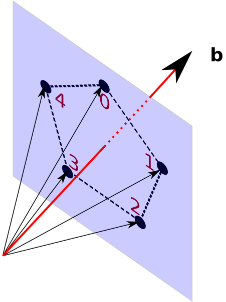
- Tensorization: If $\{e_v, b\}$ yields

$$\alpha(G) \leq \theta$$

then $\{e_v^{\otimes n}, b^{\otimes n}\}$ yields

$$\alpha(G^n) \leq \theta^n$$

Lovász' miracle



- Punchline: Find good representation $\{e_v\}$ and handle b, then

$$C(G) \leq \frac{1}{\min_{v \in V(G)} (e_v, b)^2} .$$

- So: $C(C_5) \leq \frac{1}{2} \log 5$
- Generally not tight, but for the pentagon (magically).

New upper bound (converse)

Problem setup

Definition

Define semi-metric on G:

$$d(g, g') = \begin{cases} 0, & g = g' \\ 1, & g \sim g' \\ \infty, & g \not\sim g' \end{cases}$$

and extend to G^n: $d(\mathbf{g}, \mathbf{g}') = \sum_i d(g_i, g_i')$. Then

$$R^*(\delta) \triangleq \limsup_n \frac{1}{n} \log \max\{|S| : d_{min}(S) \geq \delta n\}$$

Problem setup

Definition

Define semi-metric on G:

$$d(g,g') = \begin{cases} 0, & g = g' \\ 1, & g \sim g' \\ \infty, & g \not\sim g' \end{cases}$$

and extend to G^n: $d(\mathbf{g},\mathbf{g}') = \sum_i d(g_i, g_i')$. Then

$$R^*(\delta) \triangleq \limsup_n \frac{1}{n} \log \max\{|S| : d_{min}(S) \ge \delta n\}$$

- Pentagon: $d(\mathbf{g},\mathbf{g}')$ = number of ± 1 symbol-flips needed.
- Coding theory: $A(n,d) \triangleq \max\{|S| : d_{min}(S) \ge d\}$.
- Graph theory: $A(n,d)$ = max independent set of a subgraph of G^n.
- Shannon capacity of a graph $C = R^*(1) = R^*(\infty)$

Fourier method

- Pentagon: Identify vertices with $\mathbb{F}_5^n$.
- Given $f : \mathbb{F}_5^n \to \mathbb{C}$ define Fourier transform

$$\hat{f}(\nu) \triangleq \sum_{\mathbf{x} \in \mathbb{F}_5^n} f(\mathbf{x}) \omega_5^{<\nu, \mathbf{x}>}, \qquad \omega_5 = e^{\frac{2\pi i}{5}}$$

Fourier method

- Pentagon: Identify vertices with $\mathbb{F}_5^n$.
- Given $f : \mathbb{F}_5^n \to \mathbb{C}$ define Fourier transform

$$\hat{f}(\nu) \triangleq \sum_{\mathbf{x}\in\mathbb{F}_5^n} f(\mathbf{x})\omega_5^{<\nu,\mathbf{x}>}, \qquad \omega_5 = e^{\frac{2\pi i}{5}}$$

- Suppose we found f satisfying:

$$\begin{cases} f(\mathbf{x}) \le 0, & d(0,\mathbf{x}) \ge \delta n \\ \hat{f}(\nu) \ge 0 \end{cases}$$

- ... then $\forall S \subset \mathbb{F}_5^n$ with $d_{min}(S) \ge \delta n$:

$$\begin{aligned} |S| f(\mathbf{0}) &\ge \sum_{\mathbf{s},\mathbf{s}'\in S} f(\mathbf{s}-\mathbf{s}') && (1) \\ = (f * 1_S, 1_S) &= (\hat{f}\cdot \hat{1}_S, \hat{1}_S) && (2) \\ &\ge 5^{-n}\hat{f}(\mathbf{0})|S|^2 && (3) \end{aligned}$$

Fourier method

- Pentagon: Identify vertices with $\mathbb{F}_5^n$.
- Given $f : \mathbb{F}_5^n \to \mathbb{C}$ define Fourier transform

$$\hat{f}(\nu) \triangleq \sum_{\mathbf{x} \in \mathbb{F}_5^n} f(\mathbf{x}) \omega_5^{<\nu, \mathbf{x}>}, \qquad \omega_5 = e^{\frac{2\pi i}{5}}$$

- Suppose we found f satisfying:

$$\begin{cases} f(\mathbf{x}) \le 0, & d(0, \mathbf{x}) \ge \delta n \\ \hat{f}(\nu) \ge 0 \end{cases}$$

- ... then $\forall S \subset \mathbb{F}_5^n$ with $d_{min}(S) \ge \delta n$:

$$|S| \le 5^n \frac{f(\mathbf{0})}{\hat{f}(\mathbf{0})}$$

- Now just optimize over f ...

Lovász choice

$$(*) \qquad \begin{cases} f(\mathbf{x}) \le 0, & d(0,\mathbf{x}) \ge \delta n \\ \hat{f}(\nu) \ge 0 \end{cases} \implies |S| \le 5^n \frac{f(\mathbf{0})}{\hat{f}(\mathbf{0})}$$

- Lovász's umbrella:

$$g(\mathbf{x}) \triangleq \prod_{j=1}^{n} g_1(x_j)\,, \qquad \hat{g}(\nu) = \prod_{j=1}^{n} \hat{g}_1(\nu_j)$$

$$g_1(x) = \begin{cases} 1, & x = 0 \\ \phi, & x = \pm 1, \\ 0, & x = \pm 2 \end{cases} \qquad \hat{g}_1(\nu) = \begin{cases} \sqrt{5}, & \nu = 0 \\ 1+\phi^2, & \nu = \pm 1 \\ 0, & \nu = \pm 2 \end{cases}$$

$(\phi = \frac{\sqrt{5}-1}{2})$

- Yields:

$$|S| \le (\sqrt{5})^n \qquad \text{whenever } d_{min}(S) = \infty\,.$$

Our key idea: product assignment

$$(*) \qquad \begin{cases} f(\mathbf{x}) \le 0, & d(0,\mathbf{x}) \ge \delta n \\ \hat{f}(\nu) \ge 0 \end{cases} \implies |S| \le 5^n \frac{f(\mathbf{0})}{\hat{f}(\mathbf{0})}$$

- We propose:

$$\boxed{f(\mathbf{x}) = g(\mathbf{x})h(\mathbf{x})}$$

- With constraints:

$$h(\mathbf{x}) = \begin{cases} 0, & \mathbf{x} \notin \{0, \pm 1\}^n \\ \le 0, & |\mathbf{x}| \ge \delta n \end{cases} \qquad \hat{h}(\nu) = \begin{cases} 0, & \nu \notin \{0, \pm 2\}^n \\ \ge 0, & \nu \in \{0, \pm 2\}^n \end{cases}$$

$$|S| \le 5^{2n} \frac{g(\mathbf{0})}{\hat{g}(\mathbf{0})} \cdot \frac{h(\mathbf{0})}{\hat{h}(\mathbf{0})} = 5^{\frac{3n}{2}} \frac{h(\mathbf{0})}{\hat{h}(\mathbf{0})}$$

... Delsarte's Linear Programming emerges ...

- WLOG restrict to permutation-invariant $h(\cdot)$:

$$h(\mathbf{x}) = \sum_{u=0}^{n} H(u) 1\{|\mathbf{x}| = u\}$$

- Then constraints become

$$\begin{array}{llcll} (A) & H(u) & \le & 0 & u \ge \delta n \\ (B) & H(u) & = & \sum \hat{H}(v) K_v(u) & \hat{H} \ge 0 \end{array}$$

where $K_v(\cdot)$ – Krawtchouk polynomials for "alphabet" $q = \sqrt{5}$ (i.e. orthogonal w.r.t. $\mathrm{Bino}(n, 1/\sqrt{5})$)

... Delsarte's Linear Programming emerges ...

- WLOG restrict to permutation-invariant $h(\cdot)$:

$$h(\mathbf{x}) = \sum_{u=0}^{n} H(u) 1\{|\mathbf{x}| = u\}$$

- Then constraints become

$$\begin{array}{lccll} (A) & H(u) & \leq & 0 & u \geq \delta n \\ (B) & H(u) & = & \sum \hat{H}(v) K_v(u) & \hat{H} \geq 0 \end{array}$$

where $K_v(\cdot)$ – Krawtchouk polynomials for "alphabet" $q = \sqrt{5}$ (i.e. orthogonal w.r.t. $\mathrm{Bino}(n, 1/\sqrt{5})$)

$$\min \left\{ \frac{H(0)}{\hat{H}(0)} : H \text{ s.t. (A), (B)} \right\}$$

This is exactly Delsarte's LP problem (for $q = \sqrt{5}$).

Putting it all together

Summary:

- Fourier method gives for good f:

$$|S| \le 5^n \frac{f(0)}{\hat{f}(0)}$$

- Select good $f(\cdot)$ by multiplying Lovasz' assignment:

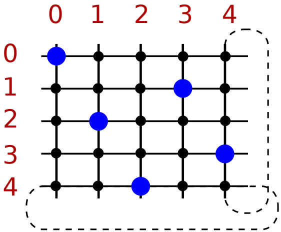
$$f(\mathbf{x}) = g_{Lovasz}(\mathbf{x})h(\mathbf{x})\,.$$

- Optimize $h(\cdot) \iff$ solve Delsarte's LP for imaginary alphabet $q = \sqrt{5}$
- Choose best known solution to get

$$R^*(\delta) \le \frac{1}{2}\log 5 + R_{LP}(\delta; \sqrt{5})$$

New lower bound (achievability)

Shannon's code: $R = \frac{1}{2}\log 5$

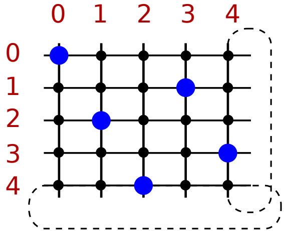


Observations:

- Shannon's code $\mathcal{C}_0$ is linear!
- Indeed it is an $\mathbb{F}_5$-span of

$$\begin{aligned} n = 2: \qquad G &= [1\ 2] \\ n = 2k: \qquad G &= [1\ 2] \otimes I_k \end{aligned}$$

Our construction

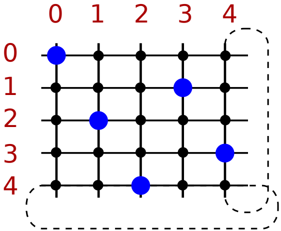


- Key idea: Choose S to be a union of cosets $\mathcal{C}_0$
- Distance between cosets:

$$\tilde{d}(x+\mathcal{C}_0, x'+\mathcal{C}_0) \triangleq \min_{c,c'\in\mathcal{C}_0} d(x+c, x+c')$$

- Note $\tilde{d}$ – metric on $\mathbb{F}_5^{2k}/\mathcal{C}_0 \approx \mathbb{F}_5^k$

Our construction



- Key idea: Choose S to be a union of cosets $\mathcal{C}_0$
- Distance between cosets:

$$\tilde{d}(x+\mathcal{C}_0, x'+\mathcal{C}_0) \triangleq \min_{c,c'\in\mathcal{C}_0} d(x+c, x+c')$$

- Note $\tilde{d}$ – metric on $\mathbb{F}_5^{2k}/\mathcal{C}_0 \approx \mathbb{F}_5^k$
- Miracle: $(\mathbb{F}_5^k, \tilde{d})$ is exactly 5-ary Hamming space!
- ... Use GV-bound for 5-ary Hamming to get:

$$R^*(\delta) \geq \frac{1}{2}\log 5 + \frac{1}{2}R_{GV}(2\delta; 5)\,.$$

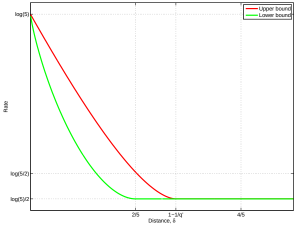
Summary: Main results

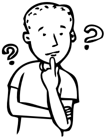
Theorem

Maximal rate $R^*(\delta)$ satisfies:

$$\frac{1}{2}\log 5 + \frac{1}{2}R_{GV}(2\delta; 5) \le R^*(\delta) \le \frac{1}{2}\log 5 + R_{LP}(\delta; \sqrt{5})\,.$$

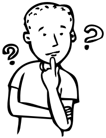
where $R_{GV}(\cdot; q)$ – q-ary Gilbert-Varshamov bound
and $R_{LP}(\cdot; q)$ – q-ary Linear-Programming bound.





Ask questions (now or later)!

Yury Polyanskiy <yp@mit.edu>



Thank you!