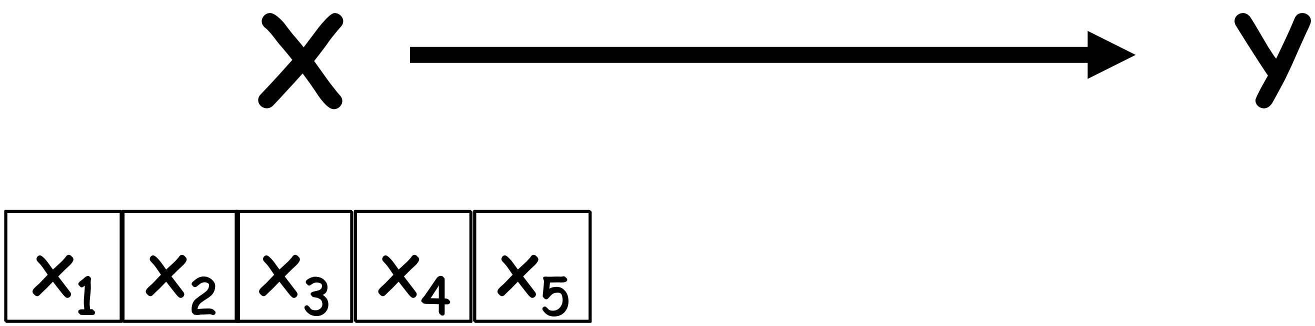
Coding for the ℓ_∞-limited Permutation Channel

Michael Langberg
SUNY Buffalo

Moshe Schwartz
Ben Gurion University

Eitan Yaakobi
Technion

Coding for Synchronization Errors



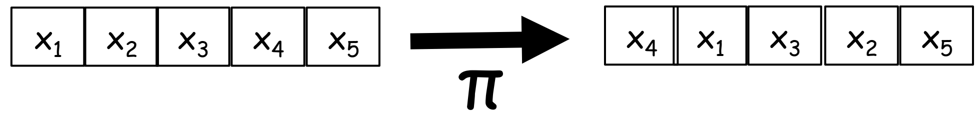
- Symbols received in incorrect order
- Channel action characterized by permutation: $\pi = \pi_1\pi_2\pi_3\pi_4\pi_5 = (4,1,3,2,5)$
- **Channel action**: $y_i = x_{\pi_i}$

Permutation Channels

$\pi = (4,1,3,2,5)$

Has been previous work on permutation channels:

- Differ on assumptions regarding possible π
- Stochastic (channel induces π governed by dist.)
- Worst-case (channel maliciously chooses worst π from set of permissible permutations)
- Differ in input (output) alphabet Σ



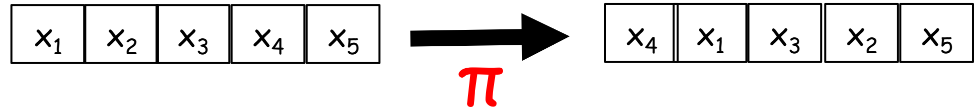
Permutation Channels

Most related previous work:

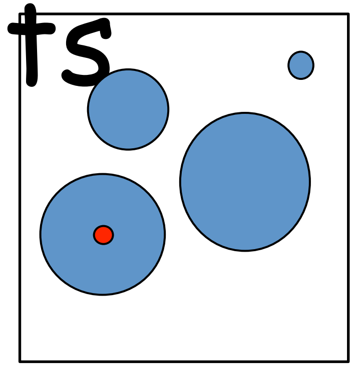
- "Bit-shift magnetic recording channel" (RLL + errors)
  - $\Sigma=\{0,1\}$
  - Limitation on π: $|i-\pi_i| \le r$ for all $x_i=1$
  - Worst case: over such π [KolesnikKrachkovsky][Ytrehus][Krachkovsky][Abdel-GhaffarWeber] …
  - Stochastic: over such π [ShamaiZehavi]

More …

- "Trapdoor channels": [BlackwellBreimanThomasian][Benjamin][AhlswedeKaspi][Chan][Kobayashi][Piret][KobayashiMorita][PermuterCuffRoyWeissman]
- Context of "rank modulation",e.g. when the codewords them selves are permutations: [KløveLinTsaiTzeng] [TamoSchwartz][ZhouSchwartzJiangBruck][Kløve][Schwartz][WangMazumdarWornell][Lehmer]
- Other models: [KovacevicVukobratovic][WalshWeber][KovacevicPopovski]



Our Model and Results



- **Model (q,r)**:
  - $|\Sigma|=q$
  - Limitation on π: bounded **ℓ_∞-distance** $= \max|i-\pi_i| \le r$
  - Worst case (combinatorial) analysis

- **Results**:
  - Set out to perform a comprehensive study
  - Error-sphere size (depends on codeword), average size
  - Upper bounds
  - Code construction (lower bounds)
  - Open Problems

$\Sigma=\{0,1\}$ and $\max_i |i-\pi_i| \leq 1$ and $n=3$

Warm Up

x_1	x_2	x_3

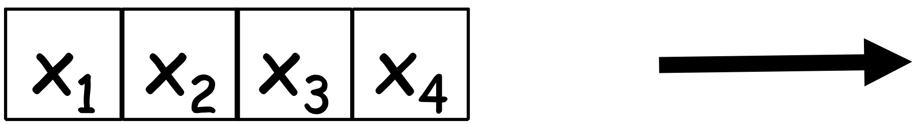
→

- **Observation**: weight of codeword does not change
- Can communicate 4 codewords: 000,001,011,111
- Rate = 2/3

- **Observation**: there exists a covering code of size 4
  - 000, 010, 101, 111
  - Covering code acts as upper bound
- Thus for n=3, rate is **2/3**

$\Sigma=\{0,1\}$ and $\max_i |i-\pi_i| \leq 1$.

Larger n?



- **Observation**: Rate R code for n=3 does not necessarily imply a rate R code for larger n
- Number of "bit errors" ($x_i \neq y_i$) increases as n increases
- **Main Goal**: What is the rate for large n?

- **Major difficulty**: error-sphere sizes
  - X GV type lower bound
  - X Naïve upper bounds

Background

- For two permutations $\pi,\sigma\in S_n$, the **ℓ_∞-distance** is
  $$d_\infty(\pi,\sigma) = \max_i|\pi(i)-\sigma(i)|$$
  $$wt_\infty(\pi) = d_\infty(\pi,Id)$$
- The **ball** of radius r centered in $x\in\Sigma^n$ is
  $$B_r(x) = \{\pi x \mid \pi\in S_n, wt_\infty(\pi) \le r\}$$
- $C\in\Sigma^n$ is an **r-ECC** if for all $c_1,c_2\in C$
  $$B_r(c_1) \cap B_r(c_2) = \emptyset$$
- **$A_q(n;r)$** = largest M s.t. there exists a length-n r-ECC of size M
- $C\in\Sigma^n$ is an **R-covering code** if
  $$\cup_{c\in C}B_R(c) = \Sigma^n$$
- **$K_q(n;R)$** = smallest M s.t. there exists a length-n R-covering code of size M

Basic Properties

- The **ℓ_∞-distance** between $x,y \in \Sigma^n$, $d_\infty(x,y)$, is the min **w** s.t. there exists $\pi \in S_n$, $wt_\infty(\pi)=w$ and $y=\pi x$
  - If such π doesn't exist then the distance is **∞**
- $n_a(x) = |\{i \in [n] : x_i=a\}|$
- $x,y \in \Sigma^n$ have **equal composition** if $n_a(x)=n_a(y)$ for all $a \in \Sigma$
- $d_\infty(x,y) = \infty$ iff x and y have different compositions
- **Lemma**: If $X \subseteq \Sigma^n$ is a set of strings with equal composition, then the ℓ_∞-distance defines a **metric** over X
- **Corollary**: C is an r-ECC if **$d_\infty(c_1,c_2) \geq 2r+1$** for all $c_1,c_2 \in C$

Basic Problems

- **Problem 1**: How to find $d_\infty(x,y)$, for $x,y \in \Sigma^n$?
- **Answer**: $d_\infty(x,y) = \max_{a\in\Sigma, j\in[n_a(x)]} |L_a(j;x) - L_a(j;y)|$ finding $\pi \in S_n$, such that $y=\pi x$ can be done in $O(n)$ time
  - $L_a(j;x)$ = the j^{th} occurrence of a in x
- **Example**:
  - $x = 00011$, $y = 01001$, $\Sigma=\{0,1\}$
  - $L_0(1;x)=1$, $L_0(2;x)=2$, $L_0(3;x)=3$, $L_1(1;x)=4$, $L_1(2;x)=5$
  - $L_0(1;x)=1$, $L_0(2;x)=3$, $L_0(3;x)=4$, $L_1(1;x)=2$, $L_1(2;x)=5$
  - $\max_{a\in\Sigma, j\in[n_a(x)]} |L_a(j;x) - L_a(j;y)| = 2$
  - $\pi = 13425$, $wt_\infty(\pi) = 2$

Basic Problems

- **Problem 2**: How to find $|B_r(x)|$?
  $B_r(x) = \{\pi x \mid \pi \in S_n\ wt_\infty(\pi) \le r\}$
  - $B_1(000) = \{000\}$, $B_1(111)=\{111\}$
  - $B_1(010) = \{100,010,001\}$, $B_1(101) = \{011,101,110\}$
- Exact sphere size depends on "run" structure of the center
- An antirun is a (maximal) sequence of different symbols
  - 011010001101 => 01.1010.0.01.101
- **Answer**: Let $P(x) = (r_1,r_2,\ldots,r_k)$ be the antirun profile, then $|B_1(x)|= \prod F_{r_i}$, where F_{r_i} is the r_i'th Fibonacci number
  - $P(0.0.0) = (1,1,1)$, $|B_1(000)| = F_1F_1F_1 = 1$
  - $P(01.10.0) = (2,2,1)$, $|B_1(01100)| = F_2F_2F_1 = 4$
    $B_1(01100) =\{01100,10100,01010,10010\}$
  - $P(0101) = (4)$, $|B_1(0101)| = F_4 = 5$
    $B_1(0101) =\{0101,1001,1010,0011,0110\}$

Basic Problems

- **Problem 2**: How to find $|B_r(x)|$?
- Exact sphere size depends on "run" structure of the center
- An antirun is a (maximal) sequence of different symbols
- **Answer**: Let $P(x) = (r_1,r_2,\ldots,r_k)$ be the antirun profile, then
  $|B_1(x)| = \prod F_{r_i}$, where F_{r_i} is the r_i'th Fibonacci number
- $\mathrm{Min}_{x\in\{0,1\}^n}|B_1(x)| = 1$
- $\mathrm{Max}_{x\in\{0,1\}^n}|B_1(x)| \leq F_n$ since $|B_r(x)| \leq |\{\pi\in S_n \mid wt_\infty(\pi) \leq r\}|$ and $|\{\pi\in S_n \mid wt_\infty(\pi) \leq 1\}| = F_n$
- $\mathrm{Max}_{x\in\{0,1\}^n}|B_1(x)| = |B_1(0101\ldots01)| = F_n$ since $F_{a+b} > F_aF_b$

Basic Problems

- **Problem 2**: How to find $|B_r(x)|$?
- Exact sphere size depends on "run" structure of the center
- An antirun is a (maximal) sequence of different symbols
- **Answer**: Let $P(x) = (r_1, r_2, \ldots, r_k)$ be the antirun profile, then
  $|B_1(x)| = \prod F_{r_i}$, where F_{r_i} is the r_i'th Fibonacci number
- $\text{Min}_{x \in \{0,1\}^n} |B_1(x)| = 1$; $\text{Max}_{x \in \{0,1\}^n} |B_1(x)| = F_n$
- $B_{r,q,n} = (1/q^n) \cdot \Sigma_{x \in Z_q^n} |B_r(x)|$
- $B_{1,q,n} = B_{1,q,n-1} + (q-1)/q \cdot B_{1,q,n-2}$
- $B_{1,q,n} = \left(\frac{\ell+\sqrt{\ell}}{2\ell}\right)\left(\frac{1+\sqrt{\ell}}{2}\right)^n + \left(\frac{\ell-\sqrt{\ell}}{2\ell}\right)\left(\frac{1-\sqrt{\ell}}{2}\right)^n$; $\ell = 5-4/q$
- $B_{1,2,n} \approx 0.789 \cdot \left(\frac{1+\sqrt{3}}{2}\right)^n$
- Can use the GV to get a lower bound on the code cardinalities
- However… we know only how to calculate $B_{1,q,n}$
- **Open Problem**: Find $|B_r(x)|$ for all x and r and $B_{r,q,n}$

Upper Bounds

- **Theorem**: For all n and r

$$A_q(n;r) \leqslant K_q(n;r) \leqslant \binom{r+q}{q-1}^{\lceil n/(r+1) \rceil}$$

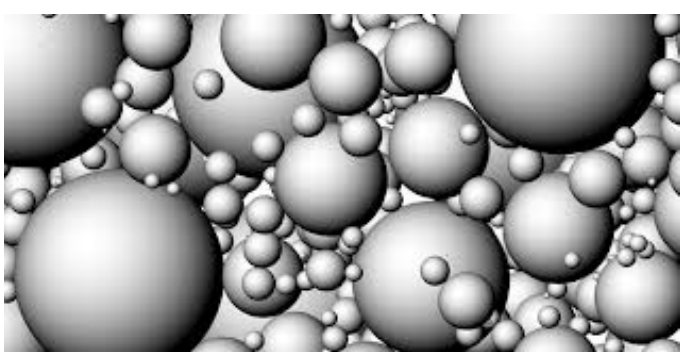
- For r=1: $A_q(n;1) \leqslant K_q(n;1) \leqslant \left[q + 2\binom{q}{2} + 2\binom{q}{3}\right]^{n/3}$
  - $A_2(n;1) \leq 4^{n/3}$
  - Results from the covering code as an upper bound
- **Problem**: Can we get a better upper bound?
- **Answer**: Yes, using a generalized sphere packing bound

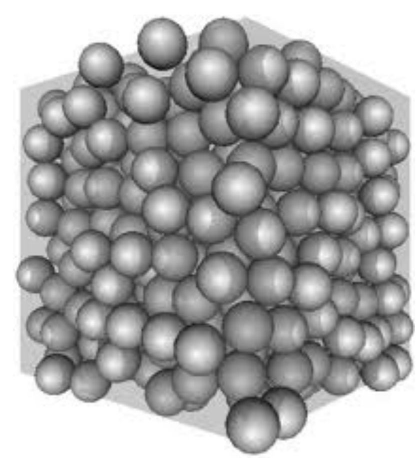
The Sphere Packing Bound

- Upper bound on a code C with min dist **2r+1**

$$|C| \leqslant \frac{2^n}{B(r)}$$

  - $B(r) = \sum_{i=0}^{r} \binom{n}{i}$
- This bound is valid for other cases as well where the error graph is regular ($|X|/\Delta_r$)
- **Q:** what happens if the graph is not regular?

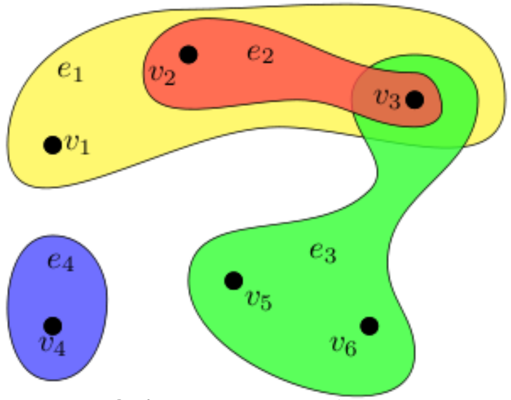




The Deletion Channel

- An example of non-regular graph
  - 10010 -> 0010, 1010, 1000, 1001
  - 11100 -> 1100, 1110
  - 10101 -> 0101, 1101, 1001, 1011, 1010
- It is not possible to apply the sphere packing bound ☹
- Previous results
  - **Levenshtein '66**: asymptotic upper bound
  - **Kulkarni & Kiyavash '12**: a method to derive explicit non-asymptotic upper bound using tools from hypergraph theory

Hypergraphs



- Let **H=(X,E)** be a **hypergraph**, where
  - $X=\{x_1,\dots,x_n\}$ – set of vertices, $E=\{E_1,\dots,E_m\}$ – set of hyperedges
  - *A* is a binary **n×m** incidence matrix of **H**
- **Matching** - a collection of pairwise disjoint hyperedges
  - **The matching number ν (H)** - size of the largest matching

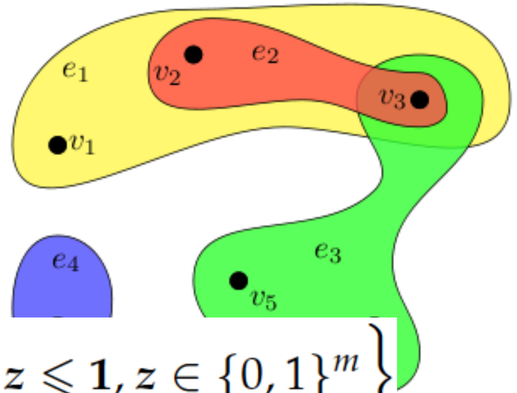
$$\nu(\mathcal{H}) = \max\left\{\sum_{i=1}^{m} z_i : A \cdot \boldsymbol{z} \leqslant \mathbf{1}, \boldsymbol{z} \in \{0,1\}^m\right\}$$

- **Transversal** - a vertices subset that intersects every hyperedge
  - **The transversal number τ(H)** - size of the smallest transversal

$$\tau(\mathcal{H}) = \min\left\{\sum_{i=1}^{n} w_i : A^T \cdot \boldsymbol{w} \geqslant \mathbf{1}, \boldsymbol{w} \in \{0,1\}^n\right\}$$

- These problems satisfy weak duality **ν (H) ≤ τ(H)**

Hypergraphs



- The matching number $\nu(\mathcal{H}) = \max\left\{\sum_{i=1}^{m} z_i : A \cdot \mathbf{z} \leqslant \mathbf{1}, \mathbf{z} \in \{0,1\}^m\right\}$
- The transversal number $\tau(\mathcal{H}) = \min\left\{\sum_{i=1}^{n} w_i : A^T \cdot \mathbf{w} \geqslant \mathbf{1}, \mathbf{w} \in \{0,1\}^n\right\}$
- These problems satisfy weak duality **$\nu(H) \leq \tau(H)$**
- The relaxation versions of these problems

$$\tau^*(\mathcal{H}) = \min\left\{\sum_{i=1}^{n} w_i : A^T \cdot \mathbf{w} \geqslant \mathbf{1}, \mathbf{w} \in \mathbb{R}_+^n\right\}$$

$$\nu^*(\mathcal{H}) = \max\left\{\sum_{i=1}^{m} z_i : A \cdot \mathbf{z} \leqslant \mathbf{1}, \mathbf{z} \in \mathbb{R}_+^m\right\}$$

satisfy strong duality

$$\nu(\mathcal{H}) \leqslant \nu^*(\mathcal{H}) = \tau^*(\mathcal{H}) \leqslant \tau(\mathcal{H})$$

- Every vector **w** in **$\tau^*(H)$** is called a ***fractional transversal***

The Deletion Channel – KK'12

- Define a hypergraph H(X,E):
  - $X = \{0,1\}^{n-1}$, E = {all 2^n single-deletion balls}
- Every single-deletion correcting code of length n is a matching in the hypergraph H
- Find the value of **τ*(H)** or any fractional transversal to get an explicit upper bound

$$\nu(\mathcal{H}) \leqslant \nu^*(\mathcal{H}) = \tau^*(\mathcal{H}) \leqslant \tau(\mathcal{H})$$

n	$\lfloor$Lev–UB$\rfloor$	$\lfloor\frac{2^n-2}{n-1}\rfloor$	$\lfloor$LP–UB$\rfloor$	$\lvert VT_0(n)\rvert$
1	1	–	1	1
2	3	2	2	2
3	4	3	2	2
4	6	4	4	4
5	10	7	6	6
6	18	12	10	10
7	34	21	17	16
8	58	36	30	30
9	103	63	53	52
10	190	113	96	94
11	363	204	175	172
12	646	372	321	316
13	1182	682	593	586
14	2232	1260	1104	1096

The General Case

- **G=(X,E)** is a graph describing an error channel graph
  - **X** = the set of all possible words (transmitted and received)
  - **E** = the set of vertices pairs of dist one
    - The distance **d(x,y)** b/w **x** and **y** is the length of the shortest path from x to y (not necessarily symmetric)
  - $\mathbf{B_r(x)}$ = $\{y \in X : d(x,y) \le r\}$; $\mathbf{deg_r(x)}$ = $|B_r(x)|$
- For any r>0, $\mathbf{H(G,r)=(X_r,E_r)}$ is a hypergraph for G
  - $\mathbf{X_r=X}$, $\mathbf{E_r=\{B_r(x) : x \in X\}}$
- Every r-ECC C in G is a **matching** in H(G,r)
- $\mathbf{A_G(n,r)}$ - the max size of a length-n r-ECC in G

For every r>0:

$$A_{\mathcal{G}}(n,r) \leqslant \tau^*(\mathcal{H}(\mathcal{G},r))$$

The Generalized Sphere Packing Bound (GSPB)

GSPB for the ℓ_∞-metric

- $G=(X_{n,w},E_{n,w})$
  - $X_{n,w}$= length-n binary vectors of weight w
  - $E_{n,w}$= all radius-1 balls centered in $x \in X_{n,w}$

n	Upper Bound	Lower Bound
3	4	4
4	8	8
5	12	12
6	16	16
7	30	28
8	46	42
9	64	64
10	116	104
11	178	157
12	256	246
13	450	388
14	696	594
15	1024	930
16	1750	1454

- **Open**: Finding a closed formula for the upper bound
- Numerical results for the linear programming problem give the following values
- **Observation**: The "average" sphere packing bound is NOT a valid upper bound in this channel
  - The sphere size is $0.789 \cdot \left(\frac{1+\sqrt{3}}{2}\right)^n$
  - If it were a valid upper bound, then 0.55 will be an upper bound on the rate, which does not hold (will see later)

Code Constructions

- **Recall**: for n=3 one can achieve optimal rate of 2/3
- **Goal**: to obtain optimal constructions for large n
- Direct construction (constrained coding):
  - Used in study of bit-shift magnetic recording channel [ShamaiZehavi][Krachkovsky][KolesnikKrachkovsky][Ytrehus][Krachkovsky][Abdel-GhaffarWeber] …
  - **Idea**: Identify blocks that can be decoded sequentially
  - **More formally**: Given a set of blocks $B \subseteq \Sigma^*$, let $C_n(B) = \{b_1 b_2 \bullet\bullet\bullet b_m \mid b_1, b_2, \ldots, b_m \in B, \Sigma |b_i| = n\}$
  - The asymptotic rate is given by $\log_2 \lambda = \limsup_{n \to \infty} \frac{\log_2 |C_n(\mathcal{B})|}{n}$
    λ is the largest solution of the equation

$$\sum_{b \in \mathcal{B}} x^{-|b|} = 1$$

Code constructions

- Direct construction (constrained coding):
  - **Idea**: Identify blocks that can be decoded sequentially
  - **More formally**: Given a set of blocks $B \subseteq \Sigma^*$, let $C_n(B) = \{b_1 b_2 \bullet\bullet\bullet b_m \mid b_1, b_2, \ldots, b_m \in B, \Sigma |b_i| = n\}$
  - The asymptotic rate is given by $\log_2 \lambda = \limsup_{n \to \infty} \frac{\log_2 |C_n(\mathcal{B})|}{n}$
    λ is the largest solution of $\sum_{b \in \mathcal{B}} x^{-|b|} = 1$

  - The set $B = \{0^{3i}1 \mid 0 \leq i\}$ was used to generate a code which satisfies the RLL constraint w/ asymp rate 0.551 [Krachkovsky]

Code constructions

- Direct construction (constrained coding):
  - **Idea**: Identify blocks that can be decoded sequentially
  - **More formally**: Given a set of blocks $B \subseteq \Sigma^*$, let $C_n(B) = \{b_1 b_2 \cdots b_m \mid b_1, b_2, \ldots, b_m \in B, \Sigma|b_i|=n\}$
  - The asymptotic rate is given by $\log_2\lambda = \limsup_{n\to\infty} \frac{\log_2 |C_n(\mathcal{B})|}{n}$
    λ is the largest solution of $\sum_{b\in\mathcal{B}} x^{-|b|} = 1$
  - The set $B = \{0^{3i}1 \mid 0 \leq i\}$ was used to generate a code which satisfies the RLL constraint w/ asymp rate 0.551
- **Theorem**: The code $C_n(B)$ for $B = B_1 \cup B_2 \cup B_3 \cup B_4$ is an ECC which allows decoding in time $\Theta(n)$.
  The asymptotic rate is $\log_2\lambda$ = **0.5875**, where λ the largest solution of $x^7-3x^4-2=0$

$$\mathcal{B}_1 = \left\{0^{2+3i}1 \;\middle|\; i \geqslant 0\right\}, \quad \mathcal{B}_2 = \left\{0^{3+3i}1^4 \;\middle|\; i \geqslant 0\right\}$$
$$\mathcal{B}_3 = \left\{1^{2+3i}0 \;\middle|\; i \geqslant 0\right\}, \quad \mathcal{B}_4 = \left\{1^{3+3i}0^4 \;\middle|\; i \geqslant 0\right\}$$

Code constructions

- **Recursive construction**:
  - **The inner code**: for each $a \in Z_q$, there exists a single-ECC C_a, s.t. for each $c \in C_a$, $wt_q(c) = a$
  - **The outer code**: $C' \in Z_q^k$ – a set of vectors with distinct q-weight
  - Construct the code $C = \bigcup_{(a_1,\ldots,a_k)\in C'} C_{a_1} \times \cdots \times C_{a_k}$
- **Theorem**: The code C is a single ECC of size $\sum_{(a_1,\ldots,a_k)\in C'} \prod_{i=1}^{k} |C_{a_i}|$
- **Example**:
  - C_0={000,110}, C_1={100,111}, C'={0101…01,1010…10}
  - We get a single ECC of length 3k and cardinality $2 \cdot 2^k$ (rate= 1/3)
- **Computer search**: a code of length 24 and rate 0.65
- Using this construction, we get codes of arbitrary length and rate **0.609**, which is our best asymptotic result

Summary: Upper & Lower Bounds

- Best asymptotic construction achieves rate 0.609
- Best (long) fixed length rate is 0.65 for n=24
- Upper bound: 2/3
- **Open Problem**: Find codes with asymptotic rate > 0.609
- **Conjecture**: The best asymptotic rate is 2/3
- **Other problems**:
  - Extensions of the results and constructions for larger radii
  - Study the capacity in case there is a fraction of **p** transpositions
  - Study the problem for other families of permutations, e.g. Ulam, Kendall's tau etc.

n	Upper Bound	Lower Bound
3	4	4
4	8	8
5	12	12
6	16	16
7	30	28
8	46	42
9	64	64
10	116	104
11	178	157
12	256	246
13	450	388
14	696	594
15	1024	930
16	1750	1454

r	λ_r	$\log_2(\lambda_r)$
2	1.3286	0.4099
3	1.2450	0.3161
4	1.1956	0.2577
5	1.1628	0.2176
6	1.1395	0.1884
7	1.1220	0.1661
8	1.1084	0.1485
9	1.0987	0.1344
10	1.0887	0.1226

Tahkn Yuo!