# Codes on Permutations: Rank Modulation

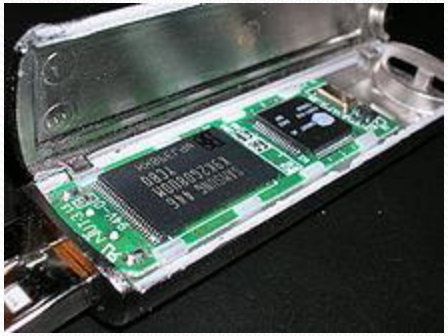

Arya Mazumdar

Joint work with Alexander Barg, University of Maryland-College Park

# Flash memory

- Array of Floating Gate Memory Cells.
- In abundant use for short-term storage and limited number of writes.
- Can they be used as caches?

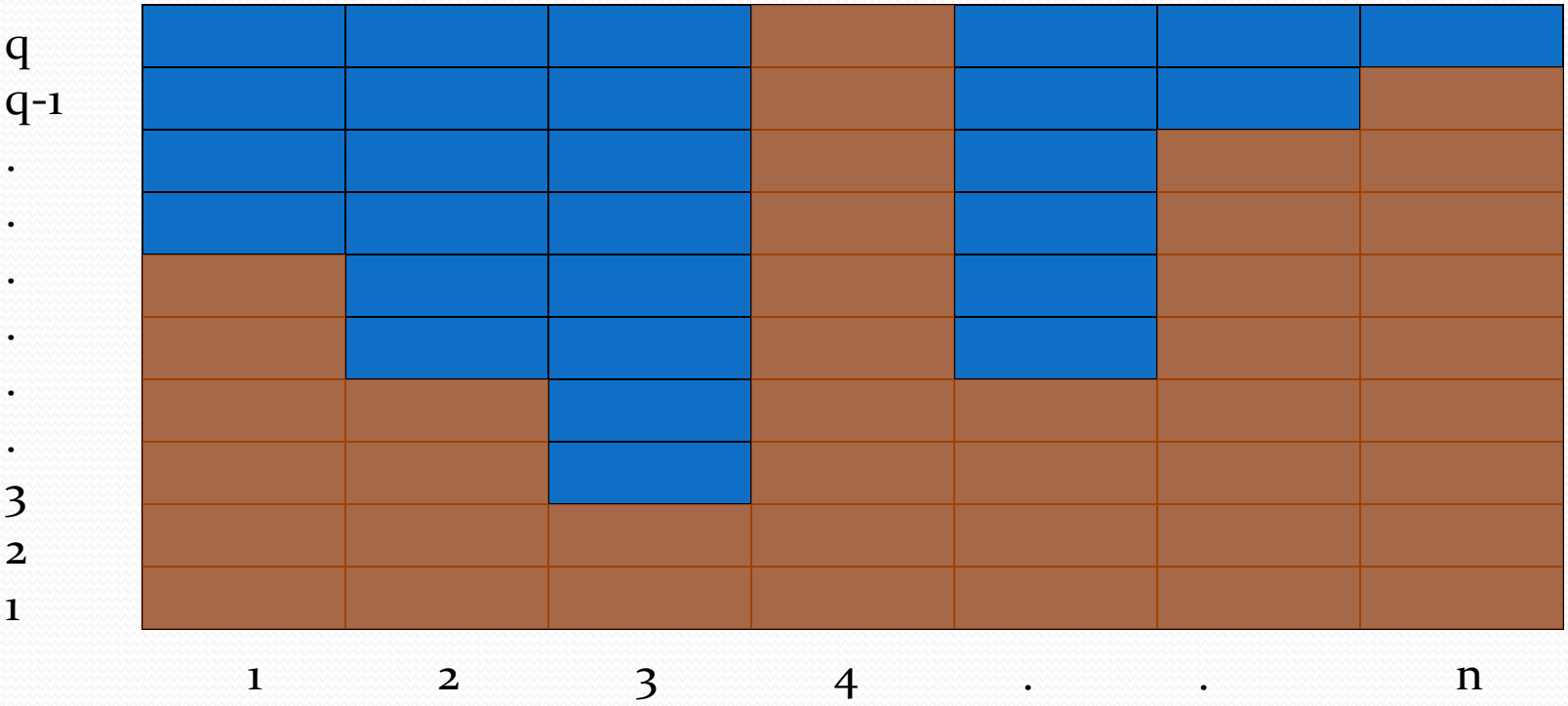
- What is the best model for the errors in Flash memory?
- How to increase the longevity of the flash devices?
- What will be the architecture of a high-performance error-resilient Flash controller?



A USB Flash Drive. The chip on the left is the flash memory. The controller is on the right (Wikipedia).

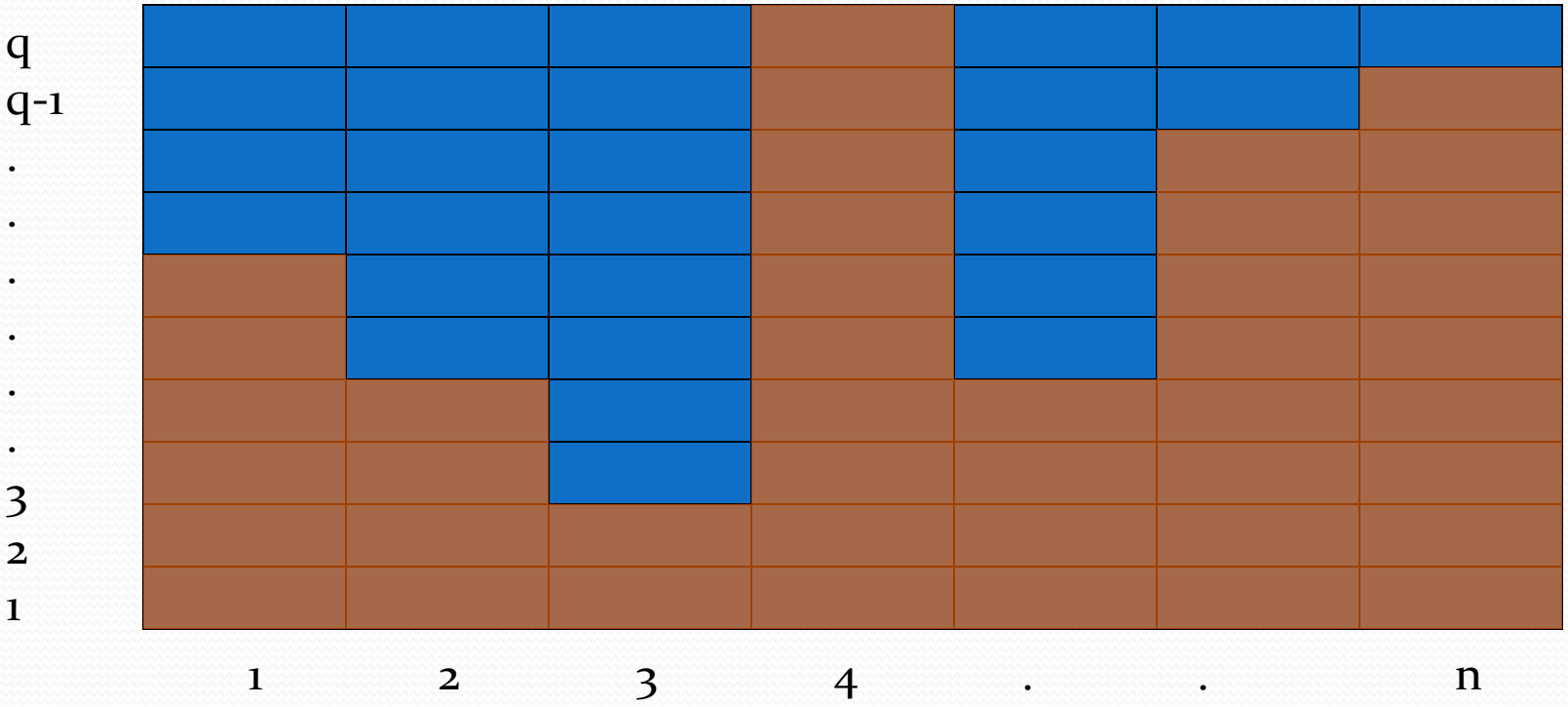
# Reliability of data in Flash memory and rank modulation scheme

Drift of charge from cells: Reliability of data stored.



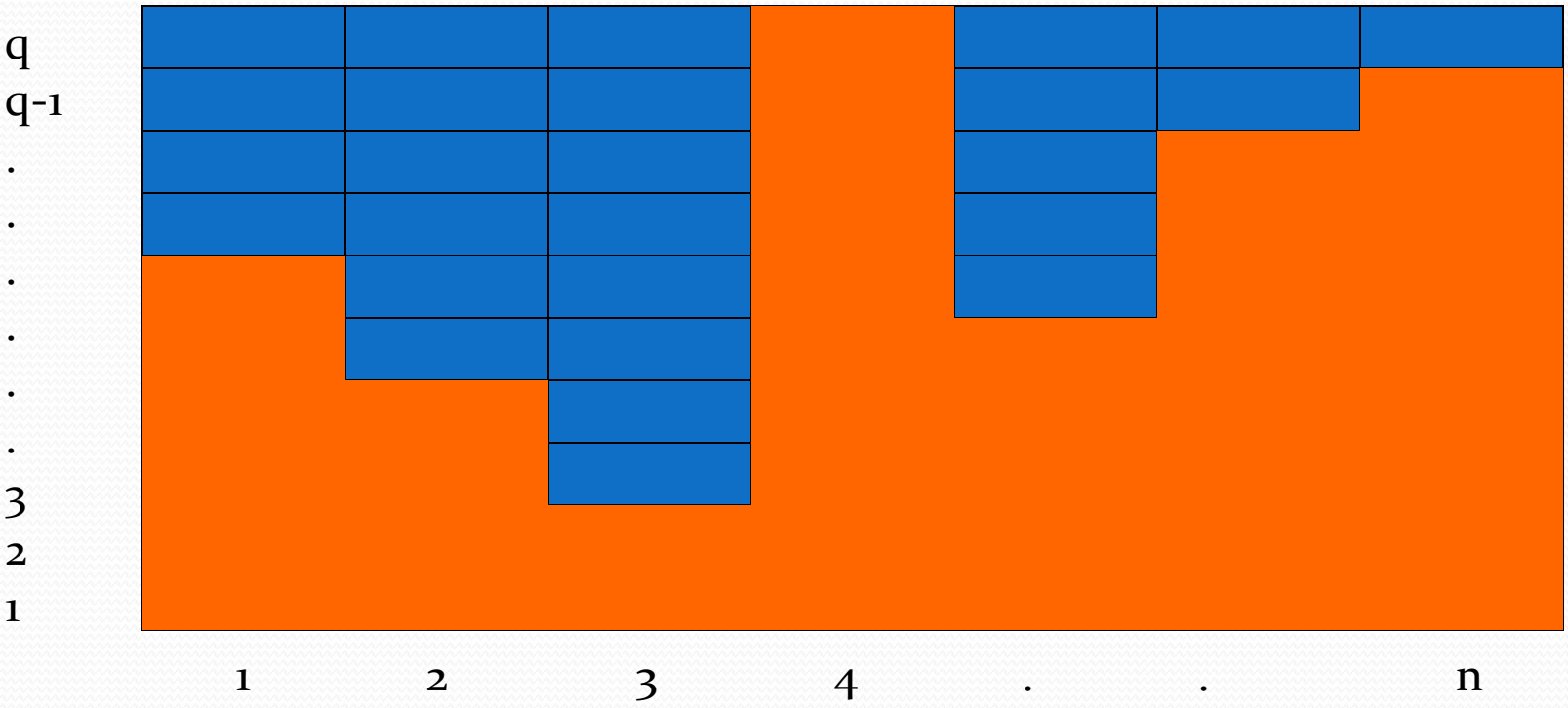

Information is written in blocks of n cells with q charge levels in each cells.

# Memory Cells




- Conventional q-ary codes can be used for protection of data.
- The error process is non-conventional!

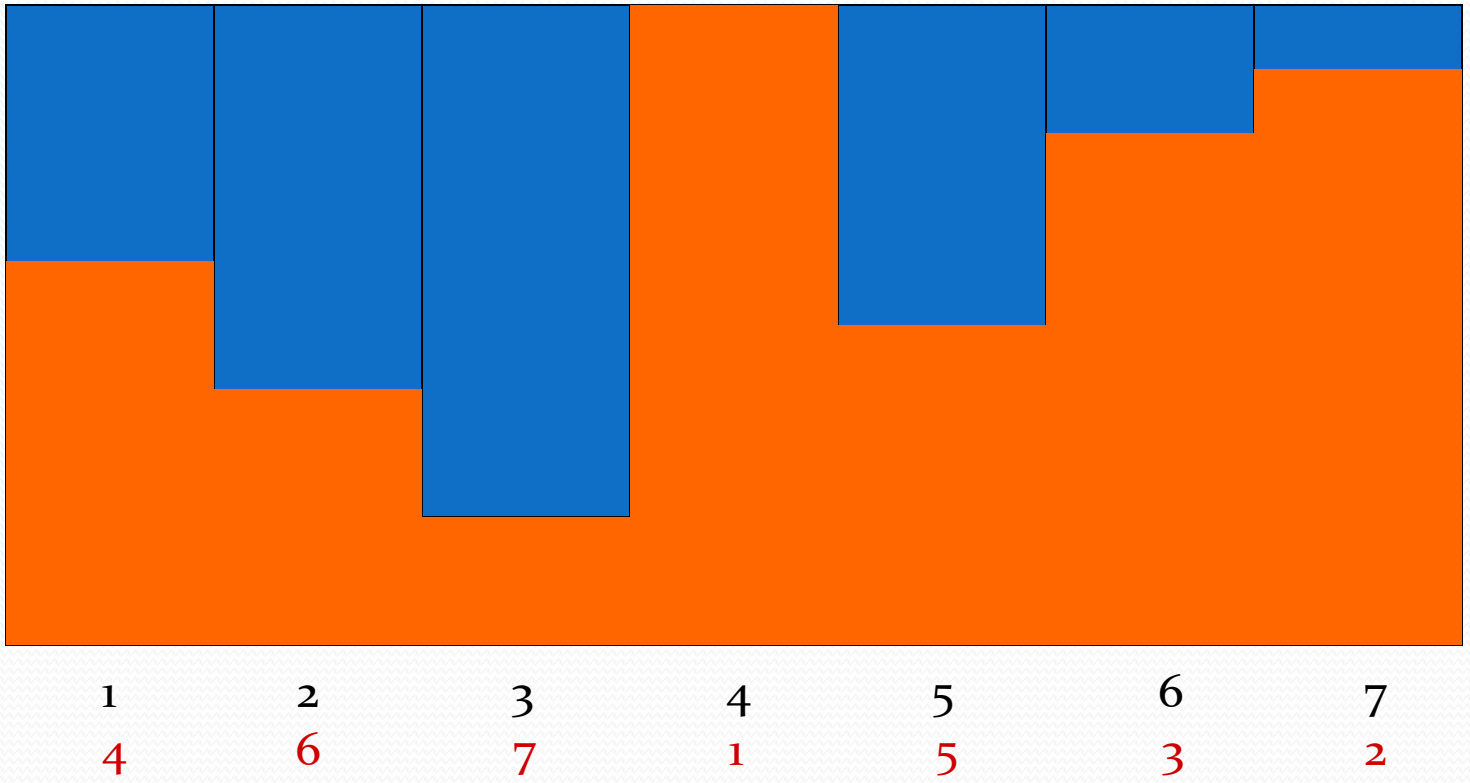
# Error caused by drift of charge




- Due to charge leakage, after some time (aging of device) all cells will contain erroneous values.
- Moreover the rate of leakage in different cells may vary.

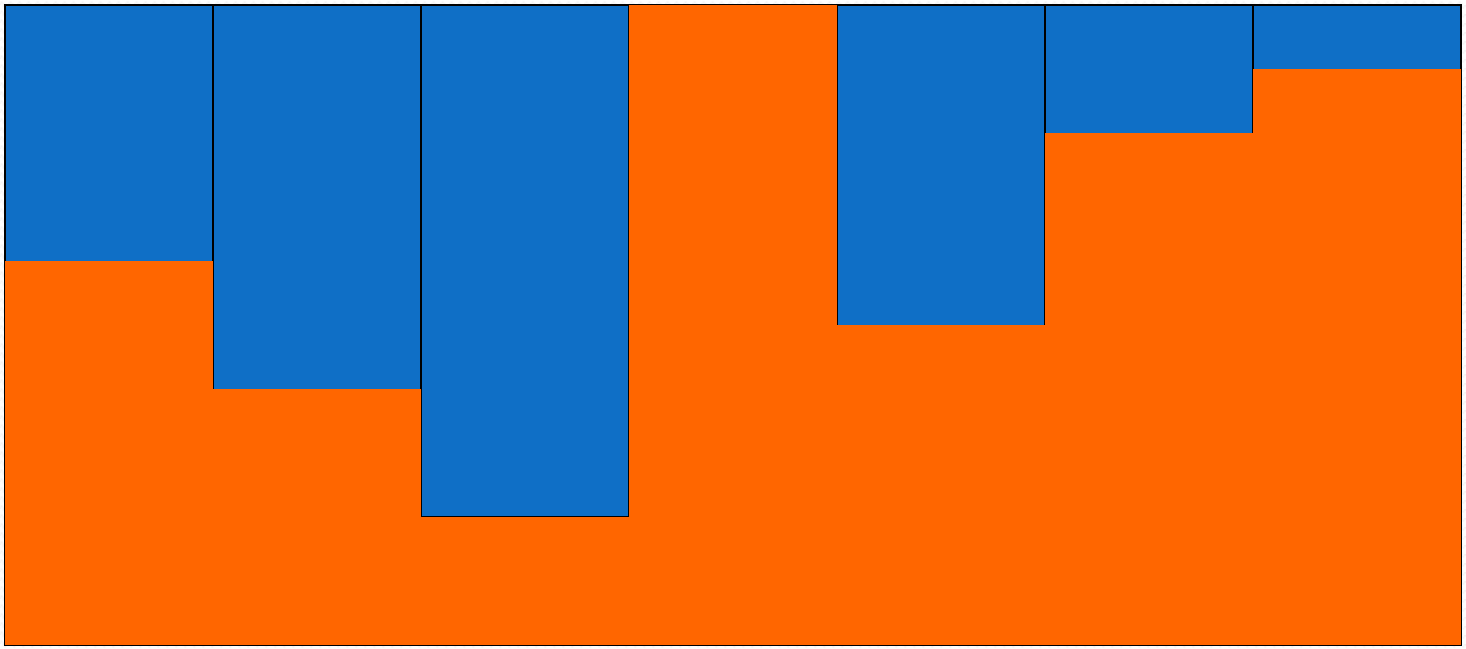
- Error correction schemes designed for q-ary writing will FAIL.

# Storing data in Flash memory



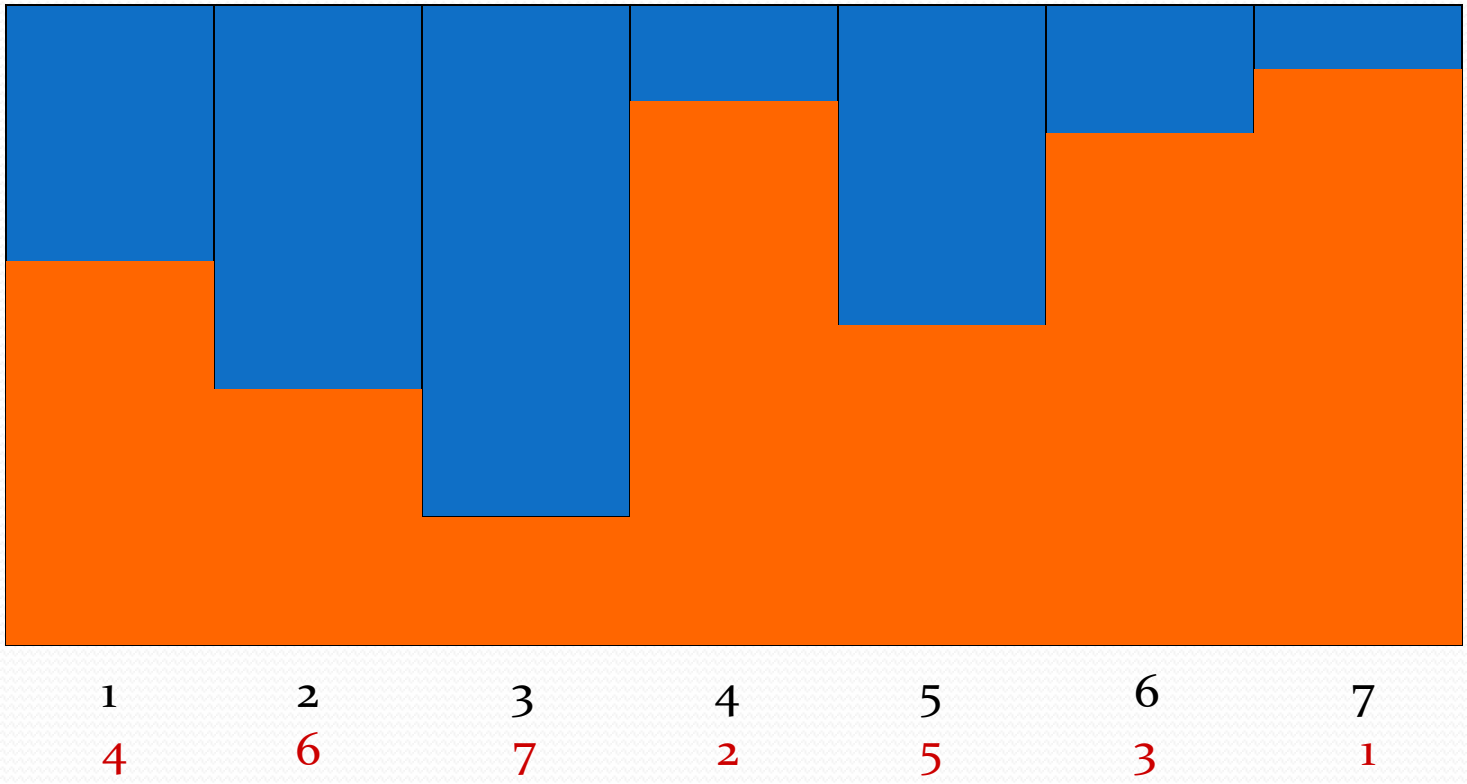

- Rank Modulation Scheme (ISIT'08 Jiang/Schwartz/Bruck).
- Store information as the relative values of the charge levels.
- $\sigma = (4, 7, 6, 1, 5, 2, 3)$
- Levels can take continuous values.

# Storing data in Flash memory




- $\sigma = (4, 7, 6, 1, 5, 2, 3)$
- $\sigma' = (7, 4, 6, 1, 5, 2, 3)$

# Storing data in Flash memory




- Error process: charge leaks.
- $$\sigma = (4, 7, 6, 1, 5, 2, 3) \rightarrow \sigma' = (7, 4, 6, 1, 5, 2, 3)$$
- Unit error : Transposition of adjacent elements.

# Codes in permutations

- $\mathbf{S}_n$= Group of permutations on n symbols
- Vector representation: $\sigma = (\sigma(1), \sigma(2), \ldots \sigma(n),)$
- Identity: (1, 2, 3, … ,n)
- Multiplication: Composition $(1, 3, 2, 4)(2, 4, 1, 3)=(2, 1, 4, 3)$
- Inverse: $(3, 4, 2, 1)(4, 3, 1, 2) = (1, 2, 3, 4)$
- Transposition: $(1,3, 5, 4, 6, 2) \mapsto (1, 3, 5, 2, 6, 4)$

- Code $\mathcal{C} \subseteq S_n$.
- Elementary errors: transpositions of adjacent symbols.

# Codes in permutations

Discrepancy measures (metrics):

- Hamming distance $d(\sigma_1, \sigma_2) = |\{i : \sigma_1(i) \neq \sigma_2(i)\}|$.
  Blake-Cohen-Deza 1979;
  Tarnanen 1989;
  Colbourn-Klove-Ling 2004;
  Cameron.
- Cayley distance (minimum number number of transpositions).
- Many more.. (Deza, Huang: "Metrics on permutations, a survey"; General literature on permutation arrays).
- Coding for Hamming distance is a well-studied problem.

# Codes in permutations with Kendall metric

Our problem: Kendall distance (Maurice Kendall, 1930s, "Advanced Statistics" Vol.1, 1946)

- $d_\tau(\sigma_1, \sigma_2)$ = minimum number of transpositions of adjacent symbols.
-

$$d_\tau((2,4,3,1),(2,3,1,4)) = 2;$$

$$(2,4,3,1) \to (2,3,4,1) \to (2,3,1,4)$$

Coding for the Kendall distance is NOT new!

Impulse Noise: H. Chadwick and L. Kurz, "Rank permutation group codes based on Kendalls correlation statistics", IEEE Trans. Inform. Theory 15, 1969.

# Rank modulation codes

- Rank Modulation Code: A set of permutations.
- Data is Encoded in to a permutation from the Code.
- Permutations are stored as relative charge levels in memory cells.
- Charge levels can be continuous.

- Unit Error: Transposition of adjacent elements.

- Want to encode as much information as possible (Large Code).
- Guarantee reliability as long as number of errors in the medium is at most a given number $t$.
- Any two code-words should be well-separated (at least by $2t + 1$).

# Coding for the Kendall distance

Properties:

- $0 \leq d_\tau(\sigma_1, \sigma_2) \leq \frac{n(n-1)}{2}$
  $d((1,2,3,4),(4,3,2,1)) = 6.$
- Right invariance: $d_\tau(\sigma_1, \sigma_2) = d_\tau(\sigma_1\sigma, \sigma_2\sigma)$ for all $\sigma_1, \sigma_2, \sigma \in S_n$.
- "Weight" of permutation $w(\sigma) = d_\tau(\sigma, e)$, $e =$ identity permutation.

# Coding for the Kendall distance

Rate of $\mathcal{C} \subseteq S_n$ :

$$R(\mathcal{C}) = \frac{\ln |\mathcal{C}|}{\ln n!}.$$

Clearly $0 \leq R \leq 1$.

Capacity of rank modulation code:

$$C(d) = \lim_{n \to \infty} \frac{\ln A(n,d)}{\ln n!}.$$

where

$$A(n,d) = \max |\mathcal{C}| : d_\tau(\mathcal{C}) \geq d.$$

- Find the maximum possible size of a rank modulation code.
- Find the exact asymptotic scaling of the distance, and then derive capacity (eg. for Hamming space for rate bounds we take $d = \delta n$).

# Bounds on the size of codes

Standard techniques of bounding the size of a code in a metric space:

- Sphere-volume bounds: Hamming bound, Gilbert-Varshamov Lower bound.
- "Independence of coordinates of codes:" Plotkin bound, Elias bound (we do not have this).
- The Kendall metric is graphic. However the metric graph is not "distance regular."
- However we have a Singleton-type bound:

$$A(n,d) \leq \left\lfloor 3/2 + \sqrt{n(n-1) - 2d + 1/4} \right\rfloor !.$$

- Not useful for capacity!

# Capacity of rank modulation Scheme

- One of the main results.

**Theorem**

$$C(d) = \begin{cases} 1 & \text{if } d = O(n) \\ 1-\epsilon & \text{if } d = \Theta(n^{1+\epsilon}),\ 0 < \epsilon < 1 \\ 0 & \text{if } d = \Theta(n^2). \end{cases}$$

The equality $C(d) = 1 - \epsilon$ holds under a slightly weaker condition, namely, $d = n^{1+\epsilon}\alpha(n)$, where $\alpha(n)$ grows slower than any positive power of $n$.

# To prove: basic arguments

- Upper bound on the size of best code (Hamming bound) : Sphere Packing.
- Lower bound on the size of best code (Gilbert-Varshamov bound) : Sphere Covering.
- Want : Volume of the sphere in Kendall Space of permutations.
- The volume does not depend on the center.

# To prove: basics of permutation

Inversion in permutation:

$$1 < 2\ 3\ 4$$
$$2 > 1\ 3\ 4$$

Inversion vector of a permutation:

| $\sigma$ | 2 | 1 | 6 | 4 | 3 | 7 | 5 | 9 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $x_\sigma$ | 0 | 1 | 0 | 1 | 2 | 0 | 2 | 0 | 1 |

- Inversion vector:

$$x_\sigma(i) = |\{j : j < i \wedge \sigma(j) > \sigma(i)\}|.$$

- $x_\sigma \in G_n \triangleq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \ldots \times \mathbb{Z}_n$.
- The mapping $S_n \rightarrow G_n$ is bijective.

# Direct attempt to find the volume of the sphere

**Proposition**

*Let $I(\sigma)$ be the total number of inversions in $\sigma$. Then*

$$w(\sigma) \triangleq d_\tau(\sigma, e) = I(\sigma) = \sum_{i=1}^{n-1} x_\sigma(i).$$

- Let $K_n(k) = |\{\sigma \in S_n : I(\sigma) = k\}|$.
- We need to find number of solutions of the equation:

$$\sum_{i=1}^{n-1} x_i = k, \quad \text{where } x_i \in \mathbb{Z}_{i+1}.$$

# Direct attempt to find the volume of the sphere

- $$K(z) = \sum_{k=0}^{\infty} K_n(k) z^k = \prod_{i=1}^{n} \frac{1 - z^i}{1 - z}.$$
- Since $K(z)$ converges for every $z$ in the finite plane, we can write

$$K_n(k) = \frac{1}{2\pi i} \oint_D \prod_{\ell=1}^{n} \left( \frac{1 - z^\ell}{1 - z} \right) z^{-k-1} dz.$$

where $D$ is a circle around the origin.

# Direct attempt to find the volume of the sphere

Margolius(2001) and Louchard and Prodinger(2003),

**Theorem**

*There exist constants $c_1$ and $c_2$ such that*

$$K_n(k) \leq \exp(c_1 n) \qquad \text{if } k = O(n),$$
$$K_n(k) = n!/\exp(c_2 n) \qquad \text{if } k = \Theta(n^2).$$

# Isometric embeddings

- $(S_n, d_\tau) \to$ Binary Hamming space of dimension $\binom{n}{2}$.

  $(i < j) \in [n] \times [n] = 1$ if $(i < j)$ forms an inversion, 0 otherwise. Chadwick, Reed (1970).

  Not useful in this context.

- Spearman's footrule: $D(\sigma_1, \sigma_2) = \sum_{i=1}^{n} |\sigma_1(i) - \sigma_2(i)|$. Diaconis, Graham (1977),

$$\frac{1}{2} D(\sigma_1, \sigma_2) \leq d_\tau(\sigma_1^{-1}, \sigma_2^{-1}) \leq D(\sigma_1, \sigma_2).$$

# Isometric embeddings

- Existence of any code $\mathcal{C} \subset S_n$ with Kendall distance $d$ must imply existence of a code $\mathcal{C}' = \{\sigma^{-1} : \sigma \in \mathcal{C}\}$ of same size that have $\ell_1$ distance at least $d$.
- On the other hand existence of any code $\mathcal{C} \subset S_n$ with $\ell_1$ distance $d$ implies the code $\mathcal{C}' = \{\sigma^{-1} : \sigma \in \mathcal{C}\}$ will have Kendall distance at least $d/2$.
- Bound volume of sphere in the Lattice $Z_n^n$ with $\ell_1$ distance (Irregular Space).
- Then use the Sphere packing and Gilbert-Varshamov type argument.

# Codes that correct t-errors

Our contribution:

**Theorem**

*Let $m = ((n-2)^{t+1} - 1)/(n-3)$, where $n-2$ is a power of a prime. There exists a $t$-error-correcting rank permutation code in $S_n$ whose size satisfies*

$$M \geq \begin{cases} n!/(t(t+1)m) & (t \text{ odd}) \\ n!/(t(t+2)m) & (t \text{ even}). \end{cases}$$

- Sphere packing bound (for constant $t$ it is easy to compute) gives $M = O(n!/n^t)$ for a code $\mathcal{C}$ in $S_n$ of length $n$ that corrects $t$ errors. We show existence within a constant factor!
- Known construction: $t = 1$ $M \geq \frac{1}{2}(n-1)!$ (Jiang, Schwartz, Bruck, ISIT 2008) (by the Varshamov-Tenenholtz construction).

# Existence of good codes: proof idea

- The symmetric group $S_n$ has a bijective mapping to $G_n = \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_n$.
- Consider $G_n$ with $\ell_1$ metric. Show:

$$d_\tau(\sigma, \pi) \geq d_{\ell_1}(\mathbf{x}_\sigma, \mathbf{x}_\pi).$$

- Show existence of a code in $G_n$ that corrects $t$ additive errors.

# Existence of good codes: proof idea

- Show: existence of a code that is a subgroup of $\mathbb{Z}_{m_t}^{n-1}$ for some $m_t \geq n$.
- Compute the average intersection of the translations of the code constructed above with $G_n$ (use Group property).
- Code $\mathcal{C}$ that corrects $t$ additive errors:

$$\forall \mathbf{x}, \mathbf{y} \in \mathcal{C},\ \mathbf{x} + \mathbf{e}_1 \neq \mathbf{x} + \mathbf{e}_2, \quad \text{if} \sum_j |e_{i,j}| \leq t,\ \text{for} i = 1, 2.$$

- The errors are "symmetric", i.e., the known constructions of asymmetric error correcting codes do not apply.

# Existence of good codes: main tool

**Theorem**

*(Bose and Chowla, 1962) Let $q$ be a power of a prime and $m = (q^{t+1} - 1)/(q - 1)$. There exist $q + 1$ integers $j_0 = 0, j_1, \ldots, j_q$ in $\mathbb{Z}_m$ such that the sums*

$$j_{i_1} + j_{i_2} + \ldots + j_{i_t} \quad (0 \leq i_1 \leq i_2 \leq \ldots \leq i_t \leq q)$$

*are all different modulo $m$.*

- Extend the above theorem so that it remains true for sums and differences.

# Existence of good codes: final step

**Theorem**

*For $1 \leq i \leq q+1$ let*

$$h_i = \begin{cases} j_{i-1} + \frac{t-1}{2}m & \text{for } t \text{ odd} \\ j_{i-1} + \frac{t}{2}m & \text{for } t \text{ even} \end{cases}$$

*where the numbers $j_i$ are given by the Bose-Chowla theorem. Let $m_t = t(t+1)m$ if $t$ is odd and $m_t = t(t+2)m$ if $t$ is even. For all $\mathbf{e} \in \mathbb{Z}^{q+1}$ such that $||\mathbf{e}|| \leq t$ the sums $\sum_{i=1}^{q+1} e_i h_i$ are all distinct and nonzero modulo $m_t$.*

- We can therefore correct "symmetric errors" is $\ell_1$ norm with a "group code."

# Explicit constructions

Permutation Polynomials: Polynomials that give bijective maps from a finite field to itself.
Main Idea: Evaluations of permutation polynomials of bounded degree forms a subset of *Reed-Solomon* code.
Problem 1: Identifying permutation polynomials calls for extensive search. *Consider special classes, such as, Linearized polynomials, Dickson polynomials, monomials.*
Problem 2: Connecting Kendall Distance with Hamming distance is difficult. *We use certain accumulator-type transformation that does the job for small distances.*

Construction from good codes of the Hamming space: We find a distance preserving Gray Map (and its variations) for the space of inversion vectors and the Hamming space of comparable size.

Remember we seek an additive error correcting code in the space of inversion vectors.

We obtain family of 'good' codes, *efficiently encodable and decodable*, that corrects up to $O(n^{1+\varepsilon})$ number of errors, for $0 \leq \varepsilon \leq 1$.

# To summarize:

- We established the exact scaling law for code rate for codes with Kendall distance $d$ (capacity of rank permutation codes).
- We proved existence of good codes (a constant factor away from the sphere packing bound) for any fixed number of Kendall errors.
- We proved other bounds. Namely, Singleton Bound:

$$A(n,d) \leq \left\lfloor 3/2 + \sqrt{n(n-1) - 2d + 1/4} \right\rfloor !.$$

- We presented explicit constructions. Example: It is possible to construct a $t$-error-correcting rank modulation code of length $n$ and size

$$\frac{2^{(n+1)\lfloor \log n \rfloor - 2^{\lfloor \log n \rfloor + 1} + 2}}{((n+1)\lfloor \log n \rfloor - 2^{\lfloor \log n \rfloor + 1} + 3)^t}.$$