PERMUTATION CODES

Ago-Erik Riet[1]
joint work with Faruk Göloğlu, Jüri Lember and Vitaly Skachek

Joint Estonian-Latvian theory days of computer science at Ratnieki

October 2014

[1] ago-erik.riet@ut.ee

Motivation

- Permutation codes (for error correction) can be used to detect and correct errors in data storage devices with rank modulation and also in power-line communications.
- In a flash memory information can be stored as electric charges of different size.
  - Suppose one storage unit consists of n cells. Then information is stored as a permutation on n elements: the relative sizes of the charges in the cells are what matter.
  - In the paradigm of rank modulation we are allowed to increase the charge of one cell so that its charge becomes the largest: "bring it to the top".
  - There are Gray codes (for listing permutations) using rank modulation for the set S_n of all permutations, i.e. we can go through all the different permutations in order, using only rank modulation. [A. Jiang , R. Mateescu , M. Schwartz , J. Bruck 2009]

Permutations and groups

- Let us denote $[n] := \{1, 2, ..., n\}$.
- A permutation (or re-ordering or 'shuffle') on n elements is a bijective mapping $\sigma : [n] \to [n]$.

permutation	two-line notation	one-line notation	disjoint cycle decomposition notation
$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 6 & 2 & 3 & 5 \end{matrix}$	123456 146235	146235	(1)(24)(365)

- Permutations on n elements form a group under composition, called S_n. Let us write $\sigma\tau$ for $\tau \circ \sigma$.

Metric spaces

- A metric space (S, d) is a set S together with a (distance) metric $d : S \times S \to \mathbb{R}_+ \cup \{0\}$ which satisfies:
  - $\forall x, y \in S : d(x, y) = d(y, x)$ (symmetry)
  - $d(x, y) = 0$ if and only if $x = y$ (not a 'pre-metric')
  - and $\forall x, y, z \in S : d(x, y) + d(y, z) \geq d(x, z)$ (triangle inequality)
- Any subset $T \subseteq S$ is still a metric space with the same metric.
- Here we are concerned with metrics which take integer values.

Codes

- A code of distance d in a metric space S is a subset $T \subseteq S$ in which all pairwise distances are at least d.
- Codes can be used for error detection and correction in data transmission or storage in which case we would also have to define encoding and decoding and what it means to introduce errors, i.e. a channel. I will not do so in this talk.
- If $S := S_n$ is endowed with a metric we call a code in this space a permutation code.
- The elements of T are called codewords. The weight of a codeword is its distance to zero, or, in the case of permutation codes to the identity permutation $e = 12...n$.

Classes of metrics

- A metric d is a graph metric if there is a (simple) graph with vertex set S such that d is the distance in the graph, i.e. the number of edges on the shortest path between two vertices.
- If S is a group and $X \subseteq S$ is a generating set, i.e. $< X \cup X^{-1} > = S$ where $X^{-1} := \{x^{-1} | x \in X\}$ then the Cayley graph is the graph with vertex set S with an edge between $s \in S$ and $t \in S$ if and only if there is an $x \in X \cup X^{-1}$ with $s = tx$, or, alternatively, $s = xt$.
- If S is a group then d is a group metric if it is the graph metric for a Cayley graph on S.

The Hamming metric

- If $S = S_1 \times S_2 \times ... \times S_n$ is a Cartesian product of sets then the Hamming metric (or Hamming distance) between $s, t \in S$ is $d_H(s,t) = \#\{i \mid s_i \neq t_i\}$.
- It is in general not a graph metric.
- If $S = S_n \subseteq [n]^n$ is the group of permutations of n elements then the Hamming distance between s and t is equal to n minus the number of 1-cycles in the cycle-representation of $s^{-1}t$.
- Example: $\mathbf{1342}$ and $\mathbf{2314}$ have distance 3: they differ in positions 1, 3 and 4.

Some concrete metrics

- Now let $S := S_n$, the permutation group on n elements and consider permutations in the one-line notation.
- The Kendall τ metric d_τ between $s, t \in S$ is the minimum number of swaps of consecutive symbols in s to obtain t.
- Example: 1342 and 2314 have distance 4:

$$1\mathbf{34}2 \to 1\mathbf{32}4 \to \mathbf{12}34 \to 2\mathbf{13}4 \to 2314$$

- The cyclic Kendall τ metric d_τ^c is similar but we can also swap the first and last symbol.
- Example: 1342 and 2314 have distance 2:

$$\mathbf{1342} \to 23\mathbf{41} \to 2314$$

Some concrete metrics

- The transposition metric d_t is similar, except we are allowed to swap any two symbols. The transposition distance between s an t is equal to n minus the number of cycles in the cycle-representation of $s^{-1}t$.
- Example: 1342 and 2314 have distance 2:

$$\mathbf{13}\mathbf{42} \to \mathbf{4}31\mathbf{2} \to 2314$$

- The Ulam metric d_U counts the minimum number of times we need to pick up a symbol and insert it somewhere else to obtain t starting with s. It is equal to n minus the length of the longest common subsequence.
- Example: the distance of 1342 and 2314 is $4 - 2 = 2$: the length of the longest common subsequence is 2: the subsequence 14 works: $\mathbf{13}\mathbf{42}$ and $23\mathbf{14}$ but also 34 works: $1\mathbf{34}2$ and $2\mathbf{31}4$

Properties of the metrics

- It is easy to check they are all metrics.
- They are all graph metrics (except the Hamming metric) since they count the number of elementary operations.
- All the permutation metrics discussed so far are left-invariant meaning $d(us, ut) = d(s, t)$ for all $u, s, t \in S_n$. In other words, they are invariant under re-naming the symbols in the same way.
- The Hamming and transposition metrics are also right-invariant meaning $d(su, tu) = d(s, t)$ for all $u, s, t \in S_n$. In other words, the are invariant under re-ordering the symbols in the same way.

More properties of the metrics

- All the metrics discussed, except the Hamming metric, are even actually group metrics (under multiplication on the left) with the generating set being respectively
  - d_τ: 2-cycles of form $(i, i+1)$
  - d_τ^c: 2-cycles of form $(i, i+1)$ and the 2-cycle $(n, 1)$
  - d_t: all 2-cycles
  - d_U: cycles of form $(i, i+1, ..., j-1, j)$

Computation of distances in these metrics

- Multiplication of permutations and taking the inverse is easy.
- It is also easy to convert between the one-line and cycle notations.
- The Hamming and transposition distances are easy to see from one of these notations.
- Question: how to efficiently compute the cyclic Kendall τ distance? I don't know...

Computation of the Kendall τ distance

- The Kendall τ distance of s and t is relatively easy to compute from the one-line notation of $s^{-1}t$:
- Notice that it is equal to the sum, over $i = 1, 2, ..., n$, of the number of symbols $j < i$ which lie on the wrong side, i.e. to the right of i. This is also called the number of inversions of the permutation $s^{-1}t$.
- The number of inversions can be found in time $O(n \log n)$. Question: can we do better for permutations?
- One approach would be divide-and-conquer, a merge sort with additional information: find the number of inversions in the left and right half of the permutation, sort the halves, and finally merge the halves, keeping track of the decrease in the total number of inversions on inserting an element.

Computation of the Ulam distance

- To compute the Ulam distance of s and t we have to find the length of the longest increasing subsequence in the one-line notation of $s^{-1}t$, (or, equivalently, just find the longest common subsequence of s and t):
- This can be done by a dynamic programming approach which is $O(n^2)$, however, there is also an $O(n \log n)$ algorithm attributed to Knuth. Question: can we do better for permutations?

Sharply transitive action and the Hamming distance

- A subgroup $G \leq S_n$ acts on the set $[n]$ which just means that $g[[n]] = [n]$ and $g(h(i)) = gh(i)$ and $e(i) = i$ for all $g, h \in G$ and all $i \in [n]$ and where e is the identity permutation $12...n$.
- The action of G is transitive if every $i \in [n]$ can be mapped to any other $j \in [n]$ by some element $g \in G$.
- The group G acts k-transitively if every ordered k-tuple of distinct numbers from $[n]$ can be mapped to any other ordered k-tuple of distinct numbers (the action is coordinate-wise).
- Finally, G acts sharply k-transitively if for every two ordered k-tuples (which could be the same) there is exactly one $g \in G$ mapping one to the other.

Sharply transitive action and the Hamming distance

- Notice that a sharply k-transitive group $G \leq S_n$ is a permutation code of Hamming distance $n - k + 1$.
- How do we see it?
  - The group G acts on $S_n \subseteq [n]^n$ by left multiplication. There are n coordinates and the action is coordinate-wise.
  - Since the action is sharp, a k-tuple is mapped to the same k-tuple by only the identity permutation $e \in G$. Since G also acts on $G \subseteq S_n$ with the same action (the action preserves G), we have that two different elements of G do not have more than $k - 1$ coordinates in common. That is, the Hamming distance is at least $n - k + 1$.

Sharply transitive action and the Hamming distance

- But there are very few sharply k-transitive groups and for only $k \leq 5$.
- Important examples include some Mathieu groups (they are some of the sporadic finite groups), $AGL(1, \mathbb{F}_q)$ and $PGL(2, \mathbb{F}_q)$.
- $AGL(1, \mathbb{F}_q)$ and $PGL(2, \mathbb{F}_q)$ correspond to respectively linear transformations $ax + b$ in $\mathbb{F}_q$ and projective fractional transformations $(ax + b)/(cx + d)$ in $\mathbb{F}_q$.

Ulam distance

- An (n, d) code: every codeword has n symbols and the minimum distance is d.
- If we puncture an (n, d) code, i.e. delete one coordinate then we have an $(n-1, d-1)$ code of the same number of codewords. This is valid for classical codes but also for Ulam codes.
- The Singleton bound is an upper bound on the size (number of codewords) based on this observation.
- It turns out that at least for some small values of n and d there are Ulam codes which satisfy the Singleton bound with equality – i.e. the codes are optimal.

Ulam distance

- The following is what we know from computer experiments about the existence of optimal (n, d) Ulam codes:

	d: 2	3	4	5	6	7
n						
4	yes					
5	yes	no				
6	yes	yes	no			
7	yes	no	no	no		
8	?	?	no	no	no	
9	?	?	?	no	no	no

Ulam distance

- Here is our knowledge about the maximum sizes of (n, d) Ulam codes:

	d: 2	3	4	5	6	7
n						
4	6					
5	24	4				
6	120	24	4			
7	720	≥ 58 and < 120	≥ 12 and < 24	4		
8	?	?	< 120	< 24	4	
9	?	?	?	< 120	< 24	2

Ulam distance

- To computer experiment, we constructed the graph on vertex set S_n with an edge if and only if the corresponding vertices are at least a distance d away.
- Now we needed to find a clique of the maximum size.
- We observed a colouring of the graph for Ulam codes such that the existence of an optimal code becomes equivalent with the property that the clique number of the graph is equal to the chromatic number.
- To have an optimal code, we need to pick exactly one vertex from each colour class such that they form a clique.
- For a non-optimal code it is enough to pick at most one vertex from each colour class.
- Finally, trying to avoid exhaustive search, we could also prove upper bounds on code size in an easier way by solving certain integer linear programs. Potentially also semi-definite programs could be of use.

Thank you!

Paldies! Aitäh!