

A DIFFERENT SORT OF GROUP CODE

Let us describe a permutation group code, based on sorting using coset leaders, but employing longer cycles rather than just transpositions. The code consists of permutations $\mathbf{x} = \langle x_0, \dots, x_{n-1} \rangle$ of $\mathbf{x}_0 = \langle 0, 1, \dots, n-1 \rangle$.

We encode by writing a permutation in a canonical form. For $2 \leq k \leq n$, let σ_k be the permutation that cycles the first k entries of \mathbf{x} to the right,

$$\sigma_k(\mathbf{x}) = \langle x_{k-1}, x_0, x_1, \dots, x_{k-2}, x_k, \dots, x_{n-1} \rangle.$$

It is easy to see how to write an arbitrary permutation $\mathbf{x} = \pi \mathbf{x}_0$ as $\pi = \sigma_2^{m_2} \dots \sigma_n^{m_n}$ with each $0 \leq m_j < j$. Recursively use the σ_j 's to cycle the j -th entry of \mathbf{x} into position.

As messages, we take integer sequences of the form $m_2 \dots m_n$ with each $0 \leq m_j < j$. This message is encoded as $\pi \mathbf{x}_0$ with $\pi = \sigma_2^{m_2} \dots \sigma_n^{m_n}$. This can be quickly done.

Now we turn to decoding. Suppose that we receive the permutation \mathbf{x} . Set $\mathbf{z}_2 = \mathbf{x}$. Inductively, for $j < n$, assume that we have $m_2 \dots m_{j-1}$ such that $\mathbf{z}_j = \sigma_{j-1}^{-m_{j-1}} \dots \sigma_2^{-m_2} \mathbf{x}$ has its first j entries $t_0 \dots t_{j-1}$ in the correct cyclic order. Compute the differences $d_0 = t_j - t_0, \dots, d_{j-1} = t_j - t_{j-1}$. Note that these are also in cyclic order. If any d_i is negative, choose m_j such that d_{m_j} is the least negative; otherwise choose m_j such that d_{m_j} is the most positive. Then set $\mathbf{z}_{j+1} = \sigma_j^{-m_j} \mathbf{z}_j$.

Finally, given $\mathbf{z}_n = \langle t_0 \dots t_{n-1} \rangle$, which will have its entries in the correct cyclic order, choose m_n such that $t_{m_n} = 0$. It follows that $\mathbf{x}_0 = \sigma_n^{-m_n} \mathbf{z}_n$, as desired.

An example is illuminating. To send the message 1032 with $n = 5$, we encode thusly:

$$\begin{aligned} \mathbf{x}_0 &= \langle 01234 \rangle \\ \sigma_5^2 \mathbf{x}_0 &= \langle 34012 \rangle \\ \sigma_4^3 \sigma_5^2 \mathbf{x}_0 &= \langle 40132 \rangle \\ \sigma_3^0 \sigma_4^3 \sigma_5^2 \mathbf{x}_0 &= \langle 40132 \rangle \\ \sigma_2^1 \sigma_3^0 \sigma_4^3 \sigma_5^2 \mathbf{x}_0 &= \langle 04132 \rangle \end{aligned}$$

and send the last vector. Decoding takes us backward through the same sequence.

If n is large, then decoding can be sped up using the fact that initial segments are always cyclically ordered.