A GROUP THEORETICAL PROBLEM INSPIRED BY THE ČERNÝ CONJECTURE

Péter P. Pálfy
Alfréd Rényi Institute of Mathematics,
Hungarian Academy of Sciences
and Eötvös University, Budapest

Ischia, April 1, 2016

The Černý Conjecture

Jan Černý, *Poznámka k homogénnym experimentom s konečnými automatmi*, Matematicko-fyzikálny Časopis **14** (1964) 208-216.

Conjecture: For any synchronizing automaton with n states there exists a synchronizing word of length at most $(n-1)^2$.

The Černý Conjecture

Jan Černý, *Poznámka k homogénnym experimentom s konečnými automatmi*, Matematicko-fyzikálny Časopis **14** (1964) 208-216.

Conjecture: For any synchronizing automaton with n states there exists a synchronizing word of length at most $(n-1)^2$.

In common algebraic terms:

Let $f_1, \ldots, f_k$ be self-maps (transformations) of the n-element set. Consider the transformation semigroup $T = \langle f_1, \ldots, f_k \rangle$ generated by them. Assume that T contains a constant map. Then there exists a product $f_{i_1} \cdots f_{i_\ell}$ of word length $\ell \leq (n-1)^2$ that is a constant map.

Černý's example

Let a be the cyclic permutation $a = (0, 1, 2, \ldots, n-1)$ and let b be the transformation mapping 0 to 1 and fixing every other element. Then the unique shortest word in a and b that gives a constant map is $ba^{n-1}ba^{n-1}b \cdots ba^{n-1}b$ of length $(n-2)n + 1 = (n-1)^2$.

Černý's example

Let a be the cyclic permutation $a = (0, 1, 2, \ldots, n-1)$ and let b be the transformation mapping 0 to 1 and fixing every other element. Then the unique shortest word in a and b that gives a constant map is $ba^{n-1}ba^{n-1}b \cdots ba^{n-1}b$ of length $(n-2)n+1 = (n-1)^2$.

Sketch of proof. Consider the images after k steps $I_k = \{0, 1, \ldots, n-1\} f_{i_1} f_{i_2} \ldots f_{i_k}$, $k = 0, 1, 2, \ldots, \ell$ and work backwards. By assumption $|I_\ell| = 1$ and $|I_{\ell-1}| > 1$. Hence the last factor collapses at least two elements of $I_{\ell-1}$, so

$$f_{i_\ell} = b,\ \ I_\ell = \{1\},\ \ I_{\ell-1} = \{0, 1\}.$$

The image of b does not contain 0, hence

$$f_{\ell-1} = a,\ \ I_{\ell-2} = \{n-1, 0\},$$

the proof continues

$$f_{\ell-2} = a,\ I_{\ell-3} = \{n-2, n-1\}.$$

These elements are fixed by b (provided $n \geq 3$), so by minimality of the word length

$$f_{\ell-3} = a,\ I_{\ell-4} = \{n-3, n-2\},$$

and so on, up till

$$f_{\ell-(n-1)} = a,\ I_{\ell-n} = \{1, 2\}.$$

Now the previous factor could not have been a, since this would mean $I_{\ell-n-1} = \{0, 1\} = I_{\ell-1}$, contradicting the minimality of the word. Hence

$$f_{\ell-n} = b,\ \{0, 2\} \subseteq I_{\ell-n-1} \subseteq \{0, 1, 2\}.$$

Continuing the same way backwards, we get the result. □

A cubic upper bound

Now we turn to the general problem. Instead of finding a global optimum, we consider the question of starting with a subset X and trying to estimate the length of a word $f_{i_1} \cdots f_{i_m}$ such that $|Xf_{i_1} \ldots f_{i_m}| < |X| = |Xf_{i_1} \ldots f_{i_{m-1}}|$.

A cubic upper bound

Now we turn to the general problem. Instead of finding a global optimum, we consider the question of starting with a subset X and trying to estimate the length of a word $f_{i_1} \cdots f_{i_m}$ such that $|Xf_{i_1} \ldots f_{i_m}| < |X| = |Xf_{i_1} \ldots f_{i_{m-1}}|$.

Define $X_j = Xf_{i_1} \ldots f_{i_j}$, $j = 0, 1, \ldots, m-1$. Let $Y_{m-1} \subseteq X_{m-1}$ be a 2-element subset collapsed by f_{i_m}, and take its preimages $Y_j \subseteq X_j$ with $Y_j f_{i_{j+1}} = Y_{j+1}$. Observe that $Y_0, \ldots, Y_{m-1}$ are pairwise distinct. Indeed, if $Y_j = Y_r$ $(0 \leq j < r \leq m-1)$, then $|Xf_{i_1} \ldots f_{i_j} f_{i_{r+1}} \ldots f_{i_m}| < |X|$ contrary to the minimality. Thus $m \leq \binom{n}{2}$, and so the length of a constant product (synchronizing word) is at most

$$(n-1)\binom{n}{2} = \frac{1}{2}n(n-1)^2.$$

Pin's observation

Jean-Éric Pin, *On two combinatorial problems arising from automata theory*, Ann. Discrete Math. **17** (1983), 535–548.

Notice that by the same reason $X_j \not\supseteq Y_r$ for $j < r$.
For aesthetical purposes it is better to consider the complements of the sets X_j, call them A_j. Moreover, instead of just 2-element sets Y_j, we may consider sets of arbitrary (but uniform size) B_j.

Now the following combinatorial problem arises:
Let $A_0, \ldots, A_{m-1}$ be finite sets of size a,
$B_0, \ldots, B_{m-1}$ sets of size b. Assume that
(0) A_i and B_i are disjoint for each $i = 0, \ldots, m-1$, but
(1) A_i and B_j have a nonempty intersection for each pair of indices $i < j$.
Give an upper bound for m.

Pin's Conjecture

Pin conjectured that under these assumptions the length of the sequence $(A_0, B_0), \ldots, (A_{m-1}, B_{m-1})$ satisfies

$$m \leq \binom{a+b}{b} = \frac{(a+b)!}{a!b!}$$

Pin's Conjecture

Pin conjectured that under these assumptions the length of the sequence $(A_0, B_0), \ldots, (A_{m-1}, B_{m-1})$ satisfies

$$m \leq \binom{a+b}{b} = \frac{(a+b)!}{a!b!}$$

In Černý's problem $a = n - |X|$, $b = 2$, so it would imply that the length of a synchronizing word is at most

$$\binom{2}{2} + \binom{3}{2} + \cdots + \binom{n}{2} = \binom{n+1}{3} = \frac{1}{6}(n^3 - n).$$

Frankl's Theorem

Péter Frankl, *An extremal problem for two families of sets*, Eur. J. Comb. **3** (1982), 125–127.

Let $A_0, \ldots, A_{m-1}$ be finite sets of size a,
$B_0, \ldots, B_{m-1}$ sets of size b. Assume that
(0) A_i and B_i are disjoint for each $i = 0, \ldots, m-1$, but
(1) A_i and B_j have a nonempty intersection for each pair of indices $i < j$.
Then

$$m \leq \binom{a+b}{b} = \frac{(a+b)!}{a!b!}$$

Frankl's Theorem

Péter Frankl, *An extremal problem for two families of sets*, Eur. J. Comb. **3** (1982), 125–127.

Let $A_0, \ldots, A_{m-1}$ be finite sets of size a,
$B_0, \ldots, B_{m-1}$ sets of size b. Assume that
(0) A_i and B_i are disjoint for each $i = 0, \ldots, m-1$, but
(1) A_i and B_j have a nonempty intersection for each pair of indices $i < j$.
Then

$$m \leq \binom{a+b}{b} = \frac{(a+b)!}{a!b!}$$

This yields the best proven general upper bound for the Černý Conjecture: $\frac{1}{6}(n^3 - n)$.

A beautiful proof

The elements that occur in any of the sets A_i, B_i ($i = 0, \ldots, m-1$) will be represented by vectors

$$\mathbf{v}_x = (1, x, x^2, \ldots, x^a) \in \mathbb{R}^{a+1}.$$

Notice that any $a+1$ of these vectors are linearly independent.

A beautiful proof

The elements that occur in any of the sets A_i, B_i ($i = 0, \ldots, m-1$) will be represented by vectors

$$\mathbf{v}_x = (1, x, x^2, \ldots, x^a) \in \mathbb{R}^{a+1}.$$

Notice that any $a+1$ of these vectors are linearly independent.
For each a-element set A_i take a normal vector $\mathbf{u}_i$ of the subspace $\langle \mathbf{v}_x \mid x \in A_i \rangle$ of codimension 1.
Notice that $\langle \mathbf{u}_i, \mathbf{v}_x \rangle = 0 \iff x \in A_i$.

A beautiful proof

The elements that occur in any of the sets A_i, B_i $(i = 0, \dots, m-1)$ will be represented by vectors

$$\mathbf{v}_x = (1, x, x^2, \dots, x^a) \in \mathbb{R}^{a+1}.$$

Notice that any $a+1$ of these vectors are linearly independent.
For each a-element set A_i take a normal vector $\mathbf{u}_i$ of the subspace $\langle \mathbf{v}_x \mid x \in A_i \rangle$ of codimension 1.
Notice that $\langle \mathbf{u}_i, \mathbf{v}_x \rangle = 0 \iff x \in A_i$.
For each b-element set B_j define a function $F_j : \mathbb{R}^{a+1} \to \mathbb{R}$ by

$$F_j(\mathbf{v}) = \prod_{x \in B_j} \langle \mathbf{v}, \mathbf{v}_x \rangle.$$

Then F_j is a homogeneous polynomial of degree b in the coordinates of $\mathbf{v}$.

A beautiful proof

The elements that occur in any of the sets A_i, B_i ($i = 0, \ldots, m-1$) will be represented by vectors

$$\mathbf{v}_x = (1, x, x^2, \ldots, x^a) \in \mathbb{R}^{a+1}.$$

Notice that any $a+1$ of these vectors are linearly independent.
For each a-element set A_i take a normal vector $\mathbf{u}_i$ of the subspace $\langle \mathbf{v}_x \mid x \in A_i \rangle$ of codimension 1.
Notice that $\langle \mathbf{u}_i, \mathbf{v}_x \rangle = 0 \iff x \in A_i$.
For each b-element set B_j define a function $F_j : \mathbb{R}^{a+1} \to \mathbb{R}$ by

$$F_j(\mathbf{v}) = \prod_{x \in B_j} \langle \mathbf{v}, \mathbf{v}_x \rangle.$$

Then F_j is a homogeneous polynomial of degree b in the coordinates of $\mathbf{v}$.
We are going to show that the functions $F_0, \ldots, F_{m-1}$ are linearly independent.

proof continued

Now B_i and A_i are disjoint, hence

$$F_i(\mathbf{u}_i) = \prod_{x \in B_i} \langle \mathbf{u}_i, \mathbf{v}_x \rangle \neq 0.$$

proof continued

Now B_i and A_i are disjoint, hence

$$F_i(\mathbf{u}_i) = \prod_{x \in B_i} \langle \mathbf{u}_i, \mathbf{v}_x \rangle \neq 0.$$

If $i < j$, then A_i and B_j have at least one common element, the corresponding vector is orthogonal to $\mathbf{u}_i$, and it also occurs in a factor in the definition of F_j, hence

$$F_j(\mathbf{u}_i) = \prod_{x \in B_j} \langle \mathbf{u}_i, \mathbf{v}_x \rangle = 0.$$

proof continued

Now B_i and A_i are disjoint, hence

$$F_i(\mathbf{u}_i) = \prod_{x \in B_i} \langle \mathbf{u}_i, \mathbf{v}_x \rangle \neq 0.$$

If $i < j$, then A_i and B_j have at least one common element, the corresponding vector is orthogonal to $\mathbf{u}_i$, and it also occurs in a factor in the definition of F_j, hence

$$F_j(\mathbf{u}_i) = \prod_{x \in B_j} \langle \mathbf{u}_i, \mathbf{v}_x \rangle = 0.$$

This shows that the functions $F_0, \ldots, F_{m-1}$ are indeed linearly independent.

proof continued

Since they are homogeneous polynomials of degree b in $a+1$ variables, their number cannot exceed the dimension of the space of these homogeneous polynomials, that is

$$m \leq \binom{a+b}{b} = \frac{(a+b)!}{a!b!}$$

□

Groups, please

Motivated by the previous arguments, I suggest the following group theoretic question:
Let $g_1, \ldots, g_k$ be permutations of the n-element set, let X and Y be subsets of the permuted elements. Find an element $g = g_{i_1} \cdots g_{i_\ell}$ in the group $G = \langle g_1, \ldots, g_k \rangle$ of smallest word length such that $Xg \supseteq Y$.

Groups, please

Motivated by the previous arguments, I suggest the following group theoretic question:
Let $g_1, \ldots, g_k$ be permutations of the n-element set, let X and Y be subsets of the permuted elements. Find an element $g = g_{i_1} \cdots g_{i_\ell}$ in the group $G = \langle g_1, \ldots, g_k \rangle$ of smallest word length such that $Xg \supseteq Y$.

Replacing the generators by their inverses, we may formulate the question by requiring $Yg \subseteq X$.
This question can also be motivated by certain puzzles.

Groups, please

Motivated by the previous arguments, I suggest the following group theoretic question:
Let $g_1, \ldots, g_k$ be permutations of the n-element set, let X and Y be subsets of the permuted elements. Find an element $g = g_{i_1} \cdots g_{i_\ell}$ in the group $G = \langle g_1, \ldots, g_k \rangle$ of smallest word length such that $Xg \supseteq Y$.

Replacing the generators by their inverses, we may formulate the question by requiring $Yg \subseteq X$.
This question can also be motivated by certain puzzles.

Replacing X by its complement — as in the Pin–Frankl argument — we may require $Yg \cap X = \emptyset$.

A Group Theoretic Conjecture

Conjecture. Let $g_1, \dots, g_k$ be permutations of the n-element set, generating a transitive permutation group G. Let A and B be subsets of the set of permuted elements. If $|A||B| < n$, then there exists a permutation $g = g_{i_1} \dots g_{i_\ell} \in G$ of word length $\ell \leq |A||B|$ such that $Ag \cap B = \emptyset$.

Note that we do not use inverses in words.

A Group Theoretic Conjecture

Conjecture. Let $g_1, \ldots, g_k$ be permutations of the n-element set, generating a transitive permutation group G. Let A and B be subsets of the set of permuted elements. If $|A||B| < n$, then there exists a permutation $g = g_{i_1} \ldots g_{i_\ell} \in G$ of word length $\ell \leq |A||B|$ such that $Ag \cap B = \emptyset$.

Note that we do not use inverses in words.

The assumption $|A||B| < n$ is necessary. Otherwise, we can take an imprimitive group, and A containing a block, B containing at least one element from each block.

A Group Theoretic Conjecture

Conjecture. Let $g_1, \ldots, g_k$ be permutations of the n-element set, generating a transitive permutation group G. Let A and B be subsets of the set of permuted elements. If $|A||B| < n$, then there exists a permutation $g = g_{i_1} \ldots g_{i_\ell} \in G$ of word length $\ell \leq |A||B|$ such that $Ag \cap B = \emptyset$.

Note that we do not use inverses in words.

The assumption $|A||B| < n$ is necessary. Otherwise, we can take an imprimitive group, and A containing a block, B containing at least one element from each block.

If $|A||B| < n$, then there is a $g \in G$ satisfying $Ag \cap B = \emptyset$. Namely, by transitivity of G, for every pair of elements $a \in A$, $b \in B$, the number of permutations $g \in G$ such that $ag = b$ is $|G|/n$, so the number of permutations $g \in G$ with $Ag \cap B \neq \emptyset$ is at most $|A||B||G|/n < |G|$.

What do I know?

Very little.

What do I know?

Very little.

There are many cases when we cannot do better than word length $|A||B|$.

What do I know?

Very little.

There are many cases when we cannot do better than word length $|A||B|$.

Example 1. If $g = (1, 2, \dots, n)$ is a full cycle, $G = \langle g \rangle$ is a cyclic group, $A = \{1, 2, \dots, a\}$, $B = \{a, 2a, \dots, ba\}$, then $Ag^{ab} \cap B = \emptyset$, and ab is the smallest exponent (word length) for which it holds.

What do I know?

Very little.

There are many cases when we cannot do better than word length $|A||B|$.

Example 1. If $g = (1, 2, \ldots, n)$ is a full cycle, $G = \langle g \rangle$ is a cyclic group, $A = \{1, 2, \ldots, a\}$, $B = \{a, 2a, \ldots, ba\}$, then $Ag^{ab} \cap B = \emptyset$, and ab is the smallest exponent (word length) for which it holds.

Example 2. Let $G = \langle (1, 2), (2, 3), (3, 4), \ldots, (n-1, n) \rangle$,
$A = \{1, 2, \ldots, a\}$, $B = \{1, 2, \ldots, b\}$, then
$g = (a, a+1)(a+1, a+2) \ldots (a+b-1, a+b)$
$(a-1, a)(a, a+1) \ldots (a+b-2, a+b-1) \ldots$
$(1, 2)(2, 3) \ldots (a, a+1)$
is (one of the) shortest words for which $Ag \cap B = \emptyset$ holds.

Small cases

The case $|A| = 1$ is trivial.

By considering lots of cases, I was able to check the validity of the conjecture for the first nontrivial case $|A| = |B| = 2$. There are many different sorts of generating permutations when the shortest word has length $4 = |A||B|$, so I could not see a general pattern for the extremal cases even for these small values of $|A|$ and $|B|$.

Nevertheless, note that $4 < \binom{2+2}{2} - 1 = 5$, so this is already an improvement of the Pin-Frankl bound

Small cases

The case $|A| = 1$ is trivial.

By considering lots of cases, I was able to check the validity of the conjecture for the first nontrivial case $|A| = |B| = 2$. There are many different sorts of generating permutations when the shortest word has length $4 = |A||B|$, so I could not see a general pattern for the extremal cases even for these small values of $|A|$ and $|B|$.

Nevertheless, note that $4 < \binom{2+2}{2} - 1 = 5$, so this is already an improvement of the Pin-Frankl bound by 1.

My dream

If the group theoretic conjecture can be proved, then one can hope to get an insight how to improve the current cubic bound on the length of a synchronizing word in Černý's Conjecture. However, since this is based on estimating the number of steps to make an image smaller, this approach cannot provide a global optimum, so it cannot yield a proof of Černý's Conjecture.

Nevertheless, it may give a bound that one needs at most cn^2/k steps to map a k-element subset to a smaller subset, and so the total length of a constant product (synchronizing word) could be estimated by

$$c\left(\frac{n^2}{n}+\frac{n^2}{n-1}+\frac{n^2}{n-2}+\ldots\frac{n^2}{3}+\frac{n^2}{2}\right)<cn^2\log n.$$

But there is a long way to go to reach this conclusion.

Thanks

I would like to thank the organizers for inviting me, and also for the excellent organization of the conference.

Thanks to all of you: Patrizia, Mercede, Mariagrazia, Carlo, Costantino, Carmine, Chiara, Serena, Maria, and Antonio.

Thanks

I would like to thank the organizers for inviting me, and also for the excellent organization of the conference.

Thanks to all of you: Patrizia, Mercede, Mariagrazia, Carlo, Costantino, Carmine, Chiara, Serena, Maria, and Antonio.

Thank you for your attention.