Matematické struktury
tutorial 3 on March 6, 2017: well-ordering from AC and reconstructing graphs by counting homomorphisms

Martin Klazar*

March 13, 2017

Recall that a *linear ordering* R on (of) a set X is a binary relation $R \subset X \times X$ that is reflexive, transitive and has the property that for each two distinct elements $a, b \in X$ exactly one of aRb and bRa holds. A *well-ordering of* X is a linear ordering of X such that every non-empty set $A \subseteq X$ has the least element, the unique element $a \in A$ such that aRb for every $b \in A$. In general we denote, as we in fact did, the least element of a nonempty subset $A \subseteq X$ in a linear ordering R on X by $\min_R(A)$.

We show that the selector function formulation of the axiom of choice implies that every set can be well-ordered; the opposite implication holds trivially as we can select from each nonempty subset its least element.

Theorem 1 *Let X be a set and $f : \{A \mid \emptyset \neq A \subseteq X\} \to X$ be a map satisfying $f(A) \in A$ for every nonempty $A \subseteq X$. Then there exists a well-ordering on X.*

Proof. We consider the set

$$\mathcal{L} = \{R \mid R \text{ is a linear ordering on some } D(R) \subseteq X\} .$$

For $R \in \mathcal{L}$ we denote by $\mathcal{D}_R$ the set of all R-downsets, i.e.

$$\mathcal{D}_R = \{A \subseteq D(R) \mid x, y \in D(R), y \in A, xRy \Rightarrow x \in A\} .$$

Let

$$\mathcal{C} = \{R \in \mathcal{L} \mid A \in \mathcal{D}_R, A \neq D(R) \Rightarrow f(X \backslash A) = \min_R(D(R) \backslash A)\} .$$

We eventually show that $\mathcal{C}$ contains a well-ordering of X.

First we show that each $R \in \mathcal{C}$ is a well-ordering of $D(R)$. For a given nonempty $B \subseteq D(R)$ we define

$$A = \{y \in D(R) \backslash B \mid x \in B \Rightarrow yRx\} .$$

*klazar@kam.mff.cuni.cz

$D(R)\backslash A$ contains B and therefore is nonempty. It is easy to see that $A \in \mathcal{D}_R$. Thus

$$y := f(X\backslash A) = \min_R (D(R)\backslash A)\ .$$

Since y is least in $D(R)\backslash A$, $D(R)\backslash A$ contains B and $B \neq \emptyset$, yRx for some and every $x \in B$. If $y \notin B$, we would get $y \in A$ which is impossible. Thus $y = x \in B$ and is the least element of B (even of the superset $D(R)\backslash A$).

Second, we show that if $R, S \in \mathcal{C}$ then S *prolongs* R or R prolongs S: $D(R) \in \mathcal{D}_S \,\&\, R \subseteq S$ or $D(S) \in \mathcal{D}_R \,\&\, S \subseteq R$. Let

$$A = \{x \in D(R) \cap D(S) \mid Rx = Sx \ \&\ R \cap (Rx \times Rx) = S \cap (Sx \times Sx)\}$$

(here $Rx = \{y \in D(R) \mid yRx\}$). So A is the set of elements determining the same downset in R and S that is moreover equally ordered by R and S. We claim that $A \in \mathcal{D}_R \cap \mathcal{D}_S$. Let $z, y, x \in X$ with $x \in A$ and yRx. Then ySx since $Rx = Sx$ and if zRy then zSy and vice versa (in both cases $y, z \in Rx = Sx$ and this set is ordered in the same way by R and S). Thus $Ry = Sy$. This set is contained in $Rx = Sx$ and so is equally ordered by R and S. Thus $y \in A$ and A is an R-downset. The argument showing that A is an S-downset is the same. Now if $D(R)\backslash A, D(S)\backslash A \neq \emptyset$ then the element $y = f(X\backslash A)$ is the R-least element in $D(R)\backslash A$ and the S-least element in $D(S)\backslash A$ and hence $Ry = A \cup \{y\} = Sy$. Also, it is clear that R and S order $A \cup \{y\}$ equally (they put the new element y at the end) and so $y \in A$, a contradiction. Thus, say, $A = D(R)$, $R \subseteq S$ and S prolongs R.

Third, we show that if $T := \bigcup \mathcal{C}$ then $T \in \mathcal{C}$, thus $\mathcal{C}$ has a unique largest element with respect to inclusion. It follows by the previous paragraph that T is a linear ordering on $D(T) = \bigcup_{R \in \mathcal{C}} D(R)$ and for $x, y \in D(T)$ we have xTy iff xRy for any $R \in \mathcal{C}$ with $x, y \in D(R)$. We check that T has the property defining $\mathcal{C}$. Let $A \subseteq D(T)$ be a T-downset different from $D(T)$. Then there is an element $b \in D(T)\backslash A$, so $b \in D(R)$ for some $R \in \mathcal{C}$. We show that $A \subseteq D(R)$. If $a \in A$ is arbitrary then $a \in D(S)$ for some $S \in \mathcal{C}$. If $D(S) \in \mathcal{D}_R$ then $a \in D(R)$. If $D(R) \in \mathcal{D}_S$ and aSb then again $a \in D(R)$, and the case bSa is not possible (as then $b \in A$). So $A \subseteq D(R)$ and $D(R)\backslash A \neq \emptyset$. Thus the element $y = f(X\backslash A)$ is the least element in $D(R)\backslash A$. By the definition of $\mathcal{C}$, y is the least element in $D(S)\backslash A$ for every $S \in \mathcal{C}$ prolonging R. It follows that y is the least element in $D(T)\backslash A$ and $T \in \mathcal{C}$.

Finally, we show that $D(T) = X$ and hence T is the desired well-ordering of X. If $D(T) \neq X$ then we may use $x = f(X\backslash D(T))$ to extend T to R by setting $D(R) = D(T) \cup \{x\}$ and yRx for every $y \in D(R)$ (i.e. we add to T the new largest element x). It is clear that $R \in \mathcal{C}$. Since R strictly contains T, we have a contradiction with the maximality of T. $\Box$

This proof is according to a write-up due to A. Pultr, which follows the book J. L. Kelley, *General Topology.*

Graph reconstruction and homomorphisms

Enough for the axiom of choice. We consider a graph-theoretical problem. A *graph* is a pair $G = (V, E) = (V(G), E(G))$ where V is a finite set of *vertices* and $E \subseteq \binom{V}{2}$ is a set of *edges*, a set of some unordered pairs of distinct vertices. Two graphs G and H are *isomorphic*, $G \cong H$, if there is a bijection $f :\ V(G) \to V(H)$ such that

$$\forall \{u, v\} \in \tbinom{V(G)}{2} :\ \{u, v\} \in E(G) \iff \{f(u), f(v)\} \in E(H) .$$

For $G = (V, E)$ and $e \in E$, $G - e := (V, E\backslash\{e\})$ and the *deck of* G, denoted by $S(G)$, is the set

$$S(G) = \{G - e \mid e \in E\}$$

of all $|E|$ graphs obtained from G by erasing one edge. If $H = (W, F)$ is another graph, we say that the decks of G and H are equal, and write $S(G) = S(H)$, if there is a bijection $\beta :\ E \to F$ such that for every $e \in E$,

$$G - e \cong H - \beta(e) .$$

Necessary condition for it is obviously that G and H have equal numbers of vertices (unless $E = F = \emptyset$) and equal numbers of edges, $|V| = |W|$ and $|E| = |F|$, but this is far from being sufficient.

Our graph-theoretical problem is:

> Is it possible to recover (reconstruct) uniquely any graph G from its deck $S(G)$? More precisely, is it true that $S(G) = S(H)$ implies $G \cong H$?

For example, if G has no edge then $S(G) = \emptyset$ and G cannot be reconstructed from $S(G)$ (we cannot determine the number of vertices). If G has just one edge then $S(G)$ is the edgeless graph with vertices V and G is uniquely reconstructed from $S(G)$ (all graphs on V with one edge are mutually isomorphic). For two or three edges there exist graphs that cannot be reconstructed from their decks:

$$G = (\{1, 2, 3, 4\},\ \{\{1, 2\},\ \{3, 4\}\}) \ \text{ and }\ H = (\{1, 2, 3, 4\},\ \{\{1, 2\},\ \{1, 3\}\})$$

are non-isomorphic but have equal decks, and the same property have

$$\begin{aligned} G &= (\{1, 2, 3, 4\},\ \{\{1, 2\},\ \{2, 3\},\ \{1, 3\}\}) \ \text{ and} \\ H &= (\{1, 2, 3, 4\},\ \{\{1, 2\},\ \{1, 3\},\ \{1, 4\}\}) . \end{aligned}$$

There is a still unresolved conjecture claiming that apart of these small examples reconstruction is always possible.

Conjecture 2 (edge reconstruction conjecture, Harary, 1964)
If the graphs G and H have at least four edges and equal decks, $S(G) = S(H)$, then $G \cong H$.

We prove a partial result towards the conjecture in a theorem that says that edge reconstruction is possible for graphs with sufficiently many edges. In the proof we make use of *graph homomorphisms.* For two graphs $G = (V, E)$ and $H = (W, F)$, a *homomorphism from G to H* is a map

$$f : V \to W \text{ such that } \{u, v\} \in E \Rightarrow \{f(u), f(v)\} \in F$$

— note that in contrast with $\cong$ we have here only an implication, images of non-edges are not restricted. Existence or non-existence of homomorphisms between two graphs, or more precisely their numbers, can express many properties of graphs and graph parameters. For example,

$$\exists \text{ homomorphism from } G \text{ to } K_3 \text{ (triangle)} \iff \chi(G) \leq 3$$

(as usual, the *chromatic number* $\chi(G)$ denotes the minimum number of colors in a proper vertex coloring of G). Graph homomorphisms are a special case of homomorphisms between relational structures which you already know. A graph $G = (V, E)$ is then understood as a relational structure on V with one binary relation $E \subseteq V \times V$ that is symmetric and irreflexive.

The theorem on edge reconstruction that we prove is due to Vladimír Müller from the Mathematical Institute of Czech Academy of Sciences in Žitná (Rye) Street in Prague (not "Ľitná" as printed in the address in the article, also "Czechoslovakia" is not with us anymore after a couple of decades — panta rhei):

- V. Müller, The edge reconstruction hypothesis is true for graphs with more than $n \cdot \log_2 n$ edges, *J. Combinatorial Theory (B)* **22** (1977), 281–283.

In the following $\log_2 x$ denotes, for $x > 0$, the binary logarithm, i.e. the $y \in \mathbb{R}$ with $2^y = x$ (and not $\log \log x$ as one might think).

Theorem 3 (Müller, 1977) *If G and H are graphs with $n \geq 6$ vertices and $m \geq 1 + n(\log_2 n - 1)$ edges and with equal decks $S(G) = S(H)$, then G and H are isomorphic.*

Proof. We may assume that $V(G) = V(H) = V$. So $|V| = n \geq 6$ and $E = E(G), F = E(H) \subseteq \binom{V}{2}$ with $|E| = |F| = m \geq 1 + n(\log_2 n - 1)$.

For $A \subseteq E$ and $e \in E, f \in F$ we consider the numbers of A-copies in G and in $G - e$:

$$N(G) := \#\{B \subseteq E \mid A \cong B\} \text{ and } N_e(G) := \#\{B \subseteq E \backslash \{e\} \mid A \cong B\} .$$

Here $A \cong B$ means that $(V, A) \cong (V, B)$. We define the numbers $N(H)$ and $N_f(H)$ in the same way, just replace E with F (but keep A a subset of E). We claim that for every $A \subseteq E$ with $A \neq E$,

$$N(G) = N(H)$$

— G and H contain equal numbers of A-copies. Proof:

$$(m - |A|)N(G) = \sum_{e \in E} N_e(G) = \sum_{f \in F} N_f(H) = (m - |A|)N(H)$$

and divide by $m - |A| > 0$. The first equality follows from counting the pairs

$$\{(e, K) \mid e \in E, K \subseteq E \text{ is an } A\text{-copy avoiding } e\}$$

first by fixing Ks and then by fixing es, this is the useful double counting trick. The third equality follows from the same double counting for H with F in place of E. The crucial second equality follows by employing the bijection $\beta : E \to F$ that witnesses $S(G) = S(H)$: $G - e \cong H - \beta(e) = H - f$ for every $e \in E$. Two isomorphic graphs trivially contain equal numbers of copies of any fixed graph L (the bijection between their vertex sets that caries the isomorphism induces a bijection between the two sets of their L-copies) and $N_e(G) = N_{\beta(e)}(H) = N_f(H)$ for every $e \in E$. Thus the two sums, over F and over E, differ only by a permutation of their summands and are equal.

We shall continue with the proof and most probably finish it (anything can happen in one week, the future still has to be born in the apeiron) in the next lecture.