Lecture 9

Last lecture:

- An alternative proof of Schützenberger's Theorem
- Detailed discussin of DU-index.

Congruences for density functions

- **The Little Fermat Theorem**: A combinatorial proof
- **Gessel's Theorem**: Bounded degree Gessel classes of (directed) graphs
- Classes of relational structures of bounded degree and finite DU-index (Fischer-M., 2003).
- **The Specker Blatter Theorem**: Classes of relational structures with relations of arity 2 and finite Specker index.

Fermat's Theorem: $a^p = a \mod p$

A combinatorial proof

- Look at the wheel W_p with p a prime. The edges connecting the center to the circle are called spikes.
- Let $f : Spikes \rightarrow [a]$ a coloring of the spikes with a colors.
  There are a^p such colorings.
- Two colorings f_1 and f_2 are equivalent of the wheel can be turned from an f_1 coloring to an f_2 coloring.
- All monochromatic colorings form singleton equivalence classes. There a such classes.
- All other equivalence classes have p members.
- Hence $a^p - a \equiv 0 \pmod{p}$. Q.E.D.

Gessel's Theorem (1984)

Theorem 1 (I. Gessel 1984)

If $\mathcal{C}$ is a Gessel class of directed graphs of degree at most d with density function $d_{\mathcal{C}}(n)$, then

$$d_{\mathcal{C}}(m+n) \equiv d_{\mathcal{C}}(m) \cdot d_{\mathcal{C}}(n) \pmod{\frac{m}{\ell}}$$

where ℓ is the least common multiple of all divisors of m not greater than d.

Gessel's Theorem (reformulated as linear modular recurrence)

Theorem 2 (I. Gessel 1984)

If $\mathcal{C}$ is a Gessel class of (directed) graphs of degree at most d, then for every m there is a $q = q(d, m) \in \mathbb{N}$ such that

$$f_{\mathcal{C}}(n+q) \equiv \sum_{i=0}^{q-1} b_i \cdot f_{\mathcal{C}}(n+i) \pmod{m}$$

with $b_0 = f_{\mathcal{C}}(q)$ and $b_i = 0 : 1 \leq i \leq q-1$.

Furthemore, $q = d!m$.

Exercise: Can you make q smaller?

Orbit of a structure

Let $\mathcal{G} \subseteq \mathcal{S}_n$ be a subgroup of the full permutation group of $[n] = \{0, \ldots, n-1\}$.

For a τ-structure $\mathfrak{A}$ over the universe $A = [n]$

- the orbit $Orb_{\mathcal{G}}(\mathfrak{A})$ is the set of different labeled structures $\sigma(\mathfrak{A})$ obtained using relabelings from $\mathcal{G}$, i.e.

$$Orb_{\mathcal{G}}(\mathfrak{A}) = \{\sigma(\mathfrak{A}) : \sigma \in \mathcal{G}\}$$

- If $\mathcal{G} = \mathcal{S}_n$, we omit it and write $Orb(\mathfrak{A})$

- $Aut_{\mathcal{G}}(\mathfrak{A})$ is the set of τ-automorphisms of $\mathfrak{A}$ which are in $\mathcal{G}$.

As $Aut_{\mathcal{G}}(\mathfrak{A}) \subseteq \mathcal{G}$ is a subgroup, we have the fundamental identity

Proposition 3
For a τ-structure $\mathfrak{A}$ over the universe $A = [n]$ and $\mathcal{G}$ a subgroup of $\mathcal{S}_n$ we have

$$| Aut_{\mathcal{G}}(\mathfrak{A}) | \cdot | Orb_{\mathcal{G}}(\mathfrak{A}) | = | \mathcal{G} |$$

Gessel's Lemma

Here the group is the cyclic group $\mathbb{Z}_m$ of cyclic permutations of $[m]$.

$[m]$ is the set $\{1, \ldots, m\}$. $m + [n]$ is the set $\{m+1, \ldots, m+n\}$.

Let $G = (V(G), E(G))$ be a graph and $A, B \subseteq V(G)$.

A is **adjacent to** B if there is an edge between A and B.

Lemma 4
Let G a graph on $[m+n]$ with degree at most d.
Let ℓ be the least common multiple of all divisors of m not greater than d.

Assume in G the sets $[m]$ and $m + [n]$ are adjacent.
Then $Orb_{\mathbb{Z}_m}(G)$ is a multiple of $\frac{m}{\ell}$.

Proof: Suppose $(i, j) \in E(G)$ with $i \in [m]$ and $j \in m + [n]$.

Let $g \in Aut_{\mathbb{Z}_m}(G)$. Then $(g(i), g(j)) = (g(i), j) \in E(G)$.

So $\mid Aut_{\mathbb{Z}_m}(G) \mid \leq d$, and $\mid Aut_{\mathbb{Z}_m}(G) \mid$ divides ℓ.

Now the lemma follows from Proposition 3. Q.E.D.

Proof of Gessel's Theorem (Theorem 1)

Step 1: As Gessel classes are closed under components,
$d_{\mathcal{C}}(m) \cdot d_{\mathcal{C}}(n)$ counts the number of graphs G on $[m+n]$
where there is no edge between $[m]$ and $m+[n]$.

Step 2: $d_{\mathcal{C}}(m+n) - d_{\mathcal{C}}(m) \cdot d_{\mathcal{C}}(n)$ counts the number of graphs
for which Gessel's Lemma applies.
Therefore $d_{\mathcal{C}}(m+n) - d_{\mathcal{C}}(m) \cdot d_{\mathcal{C}}(n) \equiv 0 \pmod{\frac{m}{\ell}}$ Q.E.D.

Bounded DU-index and bounded degree

Theorem 5 (E. Fischer and J.A. Makowsky, 2002)
Let $\mathcal{P}$ be a property of τ-structures, with finite DU-index and all its members of bounded degree d. Then

- $d_{\mathcal{P}}(n)$ *satisfies a modular recurrence relation for every m.*
- *Furthermore, if additionally all the models in $\mathcal{P}$ are connected, (hence the DU-index is 2, the function $f_{\mathcal{P}}$ satisfies the trivial recurrence relations for every m.*

Example $\overline{EQ_2CLIQUES(A)}$ shows that bounded degree cannot be dropped, even for DU-index 2 (and connected structures).

For structures of unbounded degree one needs a stronger assumption, the finiteness of the Specker-index, to be discussed later (if time permits).

Density functions and orbits

Let $\mathcal{P}$ be a class of τ-structures and
$\mathcal{P}^n$ the class of structures with universe $[n]$ in $\mathcal{P}$.

We denote by $Iso(\mathcal{P})$ the τ-isomorphims classes of $\mathcal{P}$ and denote its equivalence classes by $[\mathfrak{A}]_{\mathcal{P}}$.

The orbits $Orb(\mathfrak{A})$ and the density function $d_{\mathcal{P}}(n)$ are related by the following formula:

$$d_{\mathcal{P}}(n) = \sum_{[\mathfrak{A}]_{\mathcal{P}} \in Iso(\mathcal{P}^n)} Orb(\mathfrak{A})$$

To show that $d_{\mathcal{P}}(n) = 0 \pmod{m}$
it suffices to show that for each $\mathfrak{A} \in \mathcal{P}^n$
we have $Orb(\mathfrak{A}) = 0 \pmod{m}$.

Density functions and orbits via a subgroup

Let $\mathcal{G}$ be subgroup of $\mathcal{S}_n$.
$\mathcal{G}$ induces an equivalence relation on $\mathcal{P}$:

$$\mathfrak{A} \sim_{\mathcal{G}} \mathfrak{A}' \text{ iff there is } \sigma \in \mathcal{G} \text{ with } \sigma(\mathfrak{A}) = \mathfrak{A}'$$

We denote by $\mathcal{P}/\mathcal{G}$ the set of these equivalence classes in $\mathcal{P}^n$ and denote its equivalence classes by $[\mathfrak{A}]_{\mathcal{G}}$.

Lemma 6
The orbits $Orb_{\mathcal{G}}(\mathfrak{A})$ and the density function $d_{\mathcal{P}}(n)$ are related by the following formula:

$$d_{\mathcal{P}}(n) = \sum_{[\mathfrak{A}]_{\mathcal{G}} \in \mathcal{P}^n/\mathcal{G}} Orb_{\mathcal{G}}(\mathfrak{A})$$

To show that $d_{\mathcal{P}}(n) = 0 \pmod{m}$ it suffices to show that for each $\mathfrak{A} \in \mathcal{P}^n$ we have $Orb_{\mathcal{G}}(\mathfrak{A}) = 0 \pmod{m}$.

Degrees and orbits

Lemma 7
Let $A = [n]$ *and* $B \subseteq A$ *and* $a \in A - B$.
Let N_a^B *be the set of neighbors of* a *which are in* B.

- *Let* $S_B \subseteq \mathcal{S}_n$ *be the subgroup of permutations* σ *such that* $\sigma(a) = a$ *for every* $a \in A - B$.
- *Let* $G_B^{N_a} \subseteq S_B$ *be the subgroup of* S_B *which maps* N_a^B *onto itself.*

Then $\mid Orb_{S_B}(\mathfrak{A}) \mid$ *is divisible by* $\binom{|B|}{|N_a^B|}$.

Proof:

$$\mid G_B^{N_a} \mid \cdot \binom{\mid B \mid}{\mid N_a^B \mid} = \mid S_B \mid = \mid Aut_{S_B}(\mathfrak{A}) \mid \cdot \mid Orb_{S_B}(\mathfrak{A}) \mid =$$

$$\mid Orb_{G_B^{N_a}}(\mathfrak{A}) \mid \cdot \mid Aut_{G_B^{N_a}}(\mathfrak{A}) \mid \cdot \binom{\mid B \mid}{\mid N_a^B \mid}$$

But we have $Aut_{G_B^{N_a}}(\mathfrak{A}) = Aut_{S_B}(\mathfrak{A})$, hence the result. Q.E.D.

Choosing special values

We fix m, the modulus, and d, the degree.

We put $c = d! \cdot m$.

Lemma 8

For every $t \in \mathbb{N}$ and $0 < d_1 \leq d$ we have that m divides $\binom{t \cdot c}{d_1}$.

Proof: Write out the definitions.

$$\binom{t \cdot c}{d_1} = \binom{t \cdot d! \cdot m}{d_1} = \frac{(t \cdot d! \cdot m)!}{(t \cdot d! \cdot m - d_1)! \cdot d_1!} =$$

$$t \cdot m \cdot d! \cdot \frac{\prod_{i=1}^{d_1-1}(t \cdot m \cdot d! - i)}{d_1!} =$$

$$\frac{t \cdot m \cdot d!}{d_1 \cdot (d_1 - 1)!} \cdot \prod_{i=1}^{d_1-1}(t \cdot m \cdot d! - i) = \frac{t \cdot m \cdot d!}{d_1} \cdot \prod_{i=1}^{d_1-1} \frac{(t \cdot m \cdot d! - i)}{i}$$

Q.E.D

Connected structures, I

Recall: m is the modulus, and d the degree. $c = d! \cdot m$.

Lemma 9
For every $t \in \mathbb{N}$ and every connected $\mathfrak{A}$ with $| A | \geq t \cdot c + 1$, and for every $B \subseteq A$ with $| B | = t \cdot c$, we have that $| Orb_{S_B}(\mathfrak{A}) |$ is divisible by m.

Proof: For t, A, B as required, there is $a \in A - B$ with at d_a neighbors in B, and $1 \leq d_a \leq d$.

By Lemma 7 $| Orb_{S_B}(\mathfrak{A}) |$ is divisible by $\binom{|B|}{d_a}$.

Using Lemma 8 with $| B | = t \cdot c$ and $1 \leq d_a \leq d$, we get,
it is also divisible by m.

Connected structures, II

Now we use Lemma 6 with $\mathcal{G} = S_B$ and $\mid B \mid = t \cdot c$.

But this means that B has to be fixed **independently** of the particular structure $\mathfrak{A}$ in $\mathcal{P}^n$.

However, as all the $\mathfrak{A} \in \mathcal{P}^n$ are connected, there is always an $a \in A - B$ which has neighbors in B.

Hence, by Lemma 9, for every $\mathfrak{A} \in \mathcal{P}^n$
$\mid Orb_{S_B}(\mathfrak{A}) \mid$ is divisible by m.

Q.E.D.

Remark: *We did not use a particular $\mathcal{P}$ of finite DU-index. We only used connectedness (which implies that the DU-index is 2).*

Disconnected structures, I

Let $\mathcal{P}$ be class of structures of bounded degree d and finite D-index α.

Let $\mathcal{D}_i, i \leq \alpha$ be the DU-equivalence classes. with respect to $\mathcal{P}$.

- All the structures of degree bigger than d are in one class, say $\mathcal{D}_0$.
- $\mathcal{P}$ is also one of the classes.
  (Allowing $\mathfrak{B}$ to be empty)

m and d are still fixed and $c = m \cdot d!$.
We look now at structures with universe $[n]$.

Let $t \in \mathbb{N}$ and $B = [t \cdot c]$.

- Let $\mathcal{D}_i^0$ be those structures in $\mathcal{D}_i$ for which there is $a \in A - B$ which is connected to some $b \in B$, and
- $\mathcal{D}_i^1$ be those structures in which no such a exists.

Disconnected structures, II

We want to compute $d_i(n) = d_{\mathcal{D}_i}$ and $d_i^j(n) = d_{\mathcal{D}_i^j}$ modulo m
for each $i \leq \alpha$ and $j = 0, 1$.

Clearly, $d_i(n) = d_i^0(n) + d_i^1(n)$.

For $\mathfrak{A} \in \mathcal{D}_i^0$ we apply Lemma 7. Let d_a be the number of neighbors of a in B.

Hence, $Orb_{S_B}(\mathfrak{A})$ is divisible by $\binom{t \cdot c}{d_a}$.

By Lemma 8 $Orb_{S_B}(\mathfrak{A})$ is divisible by m,
hence $Orb(\mathfrak{A})$ and $d_i^0(n)$ are divisible by m.

Conclusion:

$$d_i(n) = d_i^0(n) + d_i^1(n) = d_i^1(n) \pmod{m}$$

Disconnected structures, III

For $\mathfrak{A} \in \mathcal{D}_i^1$ we note that $\mathfrak{A}$ can be uniquely written as

$$\mathfrak{A}_1 \sqcup \mathfrak{A}_2$$

with universes $A_1 = [t \cdot c]$ and $A_2 = \{t \cdot c + 1, \ldots, n\}$.

Fact: The equivalence class $[\mathfrak{A}_1 \sqcup \mathfrak{A}_2]$ is uniquely determined by the equivalence classes $[\mathfrak{A}_1]$ and $[\mathfrak{A}_2]$.

Now we put $t(n) = \lfloor \frac{n-1}{c} \rfloor$ and $\hat{n} = n \pmod{c}$.

Conclusion: We get, summing over all possibilities

$$d_i(n) = \sum_{j=1}^{\alpha} \mu_{i,j,m,\hat{n}} d_j(t(n)) \pmod{m}$$

Disconnected structures, IV

This gives us $(\alpha \times \alpha)$-matrices

$$M(m, \hat{n}) = (\mu_{i,j,m,\hat{n}})_{i,j}$$

Let $\bar{d}(n) = (d_1(n), \ldots, d_\alpha(n))^{tr}$.

For each $\hat{n} \in \mathbb{Z}_c$ we get now the relationship

$$\bar{d}(n) = M(m, \hat{n}) \cdot \bar{d}(t(n)) \pmod{m}$$

Using the characteristic polynomials $p_{m,\hat{n}}(\lambda)$ of all the matrices $M(m, \hat{n})$, we can now compute the required linear recurrence modulo m. Q.E.D.

Graphs of unbounded degree, I

The case of graphs of unbounded degree has several complications.

- Finite DU-index of $\mathcal{P}$ does not suffice.
  We have to make a stronger assumtion: **Finite Specker index**.

- The restriction to relations of arity at most 2 is essential.

- The proof, although similar, is considerably more complicated.

Specker index, survey

- To define the Specker index of a graph property $\mathcal{P}$ one defines a binary operation $subst(H, a, G)$ where in the pointed graph $H = (V_H, E_H, a)$ the vertex a is substituted by $G = (V_G, E_G)$.

- $DU(\mathcal{P})$-equivalence is now replaced by $subst(\mathcal{P})$-equivalence: $G_1 \sim_{\mathcal{P}} G_2$ iff for all H and $a \in V_H$ we have

$$subst(H, a, G_1) \in \mathcal{P} \text{ iff } subst(H, a, G_2) \in \mathcal{P}$$

- The Specker index of $\mathcal{P}$ is the number of $subst(\mathcal{P})$-equivalence classes.

Observation:

- The DU-index of $\mathcal{P}$ is always smaller or equal The Specker-index of $\mathcal{P}$.

- $MSOL$-definability of $\mathcal{P}$ implies finite Specker index.

Pointed structures

A pointed $\bar{R}$-structure is a pair

$$(\mathfrak{A}, a)$$

with

- $\mathfrak{A}$ an $\bar{R}$-structure and
- a an element of the universe A of $\mathfrak{A}$ or
- a an element not in A.

In $(\mathfrak{A}, a)$, we speak of the structure $\mathfrak{A}$ and the *context* a.

Substitution of structures, binary case

Given two pointed structures $(\mathfrak{A}, a)$ and $(\mathfrak{B}, b)$
over a vocabulary which contains relation symbols of arity at most 2,

The pointed structure $(\mathfrak{C}, c) = Subst((\mathfrak{A}, a), (\mathfrak{B}, b))$ is defined by:

- The universe of $\mathfrak{C}$ is $A \cup B - \{a\}$.
- The context c is given by b, i.e., $c = b$.
- For $R \in \bar{R}$ of arity 1, R^C is defined by $R^C = (R^A \cap (A - \{a\})) \cup R^B$.
- For $R \in \bar{R}$ of arity 2, R^C is defined by $R^C = (R^A \cap (A - \{a\})^2) \cup R^B \cup I$ where

$$
\begin{aligned}
I = &\{(a, x) \in A \times B : (a, b) \in R^A\} \\
\cup &\{(x, a) \in B \times A : (b, a) \in R^A\} \\
\cup &\{(x, x) \in B \times B : (a, a) \in R^A\}
\end{aligned}
$$

Specker index, definition

Let $\mathcal{C}$ be a class of $\tau = \bar{R}$-structures, where τ contains only relation symbols of arity at most 2.

We define an equivalence relation between $\bar{R}$-structures depending on $\mathcal{C}$.

(i) $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are equivalent with respect to $\mathcal{C}$,

$$\mathfrak{A}_1 \sim_{Su(\mathcal{C})} \mathfrak{A}_2$$

if for every pointed structure $(\mathfrak{S}, s)$ we have that

$$Subst((\mathfrak{S}, s), \mathfrak{A}_1) \in \mathcal{C} \text{ iff } Subst((\mathfrak{S}, s), \mathfrak{A}_2) \in \mathcal{C}$$

(ii) The *Specker index* of $\mathcal{C}$ is the number of equivalence classes of $\sim_{Su(\mathcal{C})}$.

Spececker index, properties

Proposition 10 (Specker)

Let $\mathcal{C}$ be a class of $\tau = \bar{R}$-structures, where τ contains only relation symbols of arity at most 2.

(i) *If $\mathcal{C}$ is $MSOL$-definable then $\mathcal{C}$ has finite Specker index.*

(ii) *There are continuum many classes of finite Specker index.*

In fact, $Cycle(A)$ has Specker index at most 5.

If we allow additionally modular counting quantifiers (i.e use the logic $CMSOL$), definability still implies finite Specker index.

The class of Eulerian graphs is $CMSOL$-definable but not $MSOL$-definable.

Substitution of structures, general case

We can analyse substitution in a more general contex:

Given two pointed relational τ-structures $(\mathfrak{A}, a)$ and $(\mathfrak{B}, b)$ without restrictions on the arity of the relation symbols in τ.

We form a new pointed structure

$$(\mathfrak{C}, c) = Subst((\mathfrak{A}, a), (\mathfrak{B}, b))$$

defined as follows:

- The universe of $\mathfrak{C}$ is $A \cup B - \{a\}$.
- The context c is given by b, i.e., $c = b$.
- For $R \in \bar{R}$ of arity r, R^C is defined by

$$R^C = (R^A \cap (A - \{a\})^r) \cup R^B \cup I$$

  where for every tuple in R^A which contains a, I contains all possibilities of tuples obtained by replacing these occurrences of a with (identical or differing) members of of B.

Analize the properties of this new substitution and its corresponding Specker index.

You can try variations on the definition of I.

Graphs of unbounded degree, II

Theorem 11 (Specker and Blatter, 1981)

Let $\mathcal{C}$ be a class of $\tau = \bar{R}$-structures, such that

(i) τ contains only relation symbols of arity at most 2.

(ii) $\mathcal{C}$ has finite Specker index.

Then $d_{\mathcal{C}}$ satisfies a linear modular recurrence relation.

****

The full proof of the Specker-Blatter Theorem is left as project.

So is Fischer's counterexample of arity 4.

The Specker-Blatter Theorem and Hamiltonian graphs

Let HAM be the class of graphs with universe $[n]$ which do have a Hamiltonian cycle, and let $HAM(d)$ be those graphs in HAM which have degree at most d.

- Ham has infinte Specker index, hence is not $MSOL$-definable.

  Use $Star_n$ with center a and note that $Subst(Star_m, a, E_n) = K_{m,n}$, which is hamiltonian iff $m = n$.

  Note for non-definability we used a transduction mapping $a^n b^m$ on words to Km, n, too.

- Is $HAM(d)$ $MSOL$-definable?

- As $HAM(d)$ is connected its DU-index is 2. What is its Specker index?

- Do d_{HAM} and $d_{HAM(d)}$ satisfy linear modular recurrences?

- Try to compute d_{HAM} and $d_{HAM(d)}$.

Research problems stemming from the Specker-Blatter Theorem

There are many unresolved questions here, suitable for research.

- Is the Specker-Blatter Theorem true for arity 3?

- Can we strengthen the assumption on finite Specker index such that the Specker-Blatter Theorem would work for arbitrary finite relational vocabularies?

- $subst$ is an $MSOL$-smooth operation on vocabularies with relation symbols of arity at most 2. The same holds for $fuse$.

  Explore the relationship between the operation $subst$ and $fuse$ and the geberal notion of $patch$-width.

- Analize the relationship between *recognizable* classes of structures in the sense of Courcelle, and finite Specker index (and related notions).