CEQV and CSAT
for nilpotent Maltsev algebras

Michael Kompatscher
University of Oxford

03.11.2020
Panglobal Algebra and Logic Seminar

Outline

1. We understand nilpotent algebras

   Definition, wreath-product representation, examples

2. Do we *really* understand nilpotent algebras?

   Computational problems over nilpotent algebras

3. We (conditionally) understand (some) nilpotent algebras

   intermediate complexity of CEQV, CSAT

4. Tools to better understand nilpotent algebras

   higher commutator, Fitting series

Nilpotent algebras

The term condition commutator

$\mathbf{A} = (A, (f^{\mathbf{A}})_{f \in \tau})$... algebra
Pol($\mathbf{A}$)... polynomial operations

- Let $\alpha, \beta, \gamma \in \mathrm{Con}(\mathbf{A})$.
  Then $C(\alpha, \beta; \gamma)$ ("α centralizes β module γ") if

  $$t(\bar{x}, \bar{u}) \, \gamma \, t(\bar{x}, \bar{v}) \Rightarrow t(\bar{y}, \bar{u}) \, \gamma \, t(\bar{y}, \bar{v}),$$

  for all polynomials $t \in \mathrm{Pol}(\mathbf{A})$, all $\bar{x} \, \alpha \, \bar{y}$, $\bar{u} \, \beta \, \bar{v}$.
- The *commutator* $[\alpha, \beta]$ is the smallest γ with $C(\alpha, \beta; \gamma)$.

This generalizes the commutator for groups $\mathbf{G} = (G, \cdot, e, ^{-1})$

- Let $N, M \lhd G$. Then $C(\sim_N, \sim_M; 0_G)$ iff $nm = mn \; \forall n \in N, m \in M$.
- $[\sim_N, \sim_M]$ corresponds to the normal subgroup $[N, M]$.

Nilpotent algebras

Many notions lift directly from group theory:

- An algebra $\mathbf{A}$ is *Abelian* if $[1_A, 1_A] = 0_A$.
- $\alpha \in \mathrm{Con}(\mathbf{A})$ is *central* if $[1_A, \alpha] = 0_A$
- $0_A < \alpha_1 < \alpha_2 < \cdots < \alpha_n = 1_A$ is a *central series* of $\mathbf{A}$, if $[1_A, \alpha_{i+1}] \leq \alpha_i$ for every i.
- An algebra is *(n)-nilpotent*, if it has a central series.

From now on $\mathbf{A}$ has a *Maltsev term* $m(x, y, z)$ $(m(y, x, x) \approx m(x, x, y) \approx y)$

Theorem (Herrmann '77)
A Maltsev algebra $\mathbf{A}$ is Abelian if and only if is *affine*, i.e. $\mathbf{A}$ is polynomially equivalent to a module. So $p(x_1, \ldots, x_n) = \sum_{i=1}^{n} r_i x_i + c$.

Question: Can we 'decompose' nilpotent Maltsev algebras into affine algebras, similar to nilpotent groups?

Wreath products

$\mathbf{A} = (A, (f^{\mathbf{A}})_{f\in\tau})$... Maltsev algebra
$\alpha \in \mathrm{Con}(\mathbf{A})$ with $[1_A, \alpha] = 0_A$
$\mathbf{U} = \mathbf{A}/\alpha$

Theorem (Freese, McKenzie)

Then there is an *affine* $\mathbf{L}$ and operations $\hat{f}\colon U^n \to L$ such that

$$A = L \times U$$

$$f^{\mathbf{A}}((l_1, u_1), \ldots, (l_n, u_n)) = (f^{\mathbf{L}}(l_1, \ldots, l_n) + \hat{f}(u_1, \ldots, u_n), f^{\mathbf{U}}(u_1, \ldots, u_n))$$

for all basic operations $f^{\mathbf{A}}$.

We write $\mathbf{A} \cong \mathbf{L} \otimes^T \mathbf{U}$, where $T = (\hat{f})_{f\in\tau}$.
This is a special case of a *wreath product* of the two algebras $\mathbf{L}$ and $\mathbf{U}$.

Wreath product representation of nilpotent algebras

Corollary

Let $0_A < \alpha_1 < \cdots < \alpha_n = 1_A$ be a central series of $\mathbf{A}$. Then there are affine algebras $\mathbf{L}_1, \mathbf{L}_2, \ldots, \mathbf{L}_n$, such that

$$\mathbf{A} \cong \mathbf{L}_1 \otimes \mathbf{L}_2 \otimes \cdots \otimes \mathbf{L}_n$$

Examples

- The group $\mathbb{Z}_9$ is Abelian. But also $\mathbb{Z}_9 \cong \mathbb{Z}_3 \otimes^T \mathbb{Z}_3$, with

$$(l_1, l_2) +_{\mathbb{Z}_9} (m_1, m_2) = (l_1 + m_2 + \hat{c}(l_2, m_2), l_2 + m_2)$$

  where $\hat{c}(l_2, m_2) = 1$ if $l_2 + m_2 \geq 3$ and $\hat{c}(l_2, m_2) = 0$ else.
- The ring $(\mathbb{Z}_8, +, \star)$ with $x \star y = 2xy$ is 3-nilpotent:

$$(\mathbb{Z}_8, +, \star) = \mathbb{Z}_2 \otimes \mathbb{Z}_2 \otimes \mathbb{Z}_2$$

  with $(l_1, l_2, l_3) \star (m_1, m_2, m_3) = ((l_2 \cdot m_2), (l_3 \cdot m_3), 0)$.
  In general, a ring is n-nilpotent, iff $x_1 \cdot x_2 \cdots x_{n+1} \approx 0$.

Examples of nilpotent Maltsev algebras

- The loop $L_6 = \mathbb{Z}_2 \otimes^T \mathbb{Z}_3$ with $(l_1, u_1) \cdot (l_2, u_2) = (l_1 + l_2 + \hat{\phi}(u_1, u_2), u_1 + u_2)$, with

$\hat{\phi}$	0	1	2
0	0	0	0
1	0	0	0
2	0	0	1

- In every $\mathbf{A} \cong \mathbf{L}_1 \otimes \mathbf{L}_2 \otimes \cdots \otimes \mathbf{L}_n$, with constant $0 \in A$, $x \cdot y := m(x, 0, y)$ is a loop multiplication with neutral element $0 \in A$, since:

$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) =$$
$$(a_1 + b_1 + \hat{\phi}_1(a_2, b_2, \ldots, a_n, b_n), \ldots, a_{n-1} + b_{n-1} + \hat{\phi}_{n-1}(a_n, b_n), a_n + b_n)$$

Model algebras $\mathbf{A}_{p_1,\ldots,p_n}$

Let $p_1, \ldots, p_n$ be a list of primes. Then
$\mathbf{A}_{p_1,\ldots,p_n} := \mathbb{Z}_{p_1} \otimes \mathbb{Z}_{p_2} \otimes \cdots \otimes \mathbb{Z}_{p_n}$, with operations $+$, $f_1, \ldots, f_{n-1}$

- $+$ component-wise addition
- $f_1, \ldots, f_{n-1}$ unary, with $f_i((l_1, l_2, \ldots, l_n)) = (0, \ldots, \underbrace{\hat{f}_i(l_{i+1})}_{i}, 0, \ldots 0)$

$$\hat{f}_i(l_{i+1}) = \begin{cases} 1 \text{ if } l_{i+1} = 0 \\ 0 \text{ else.} \end{cases}$$

- For every $\hat{p} : \mathbb{Z}^m_{p_{i+1}} \to \mathbb{Z}_{p_i}$ in the *linear closed clonoid* generated by $\hat{f}_i$ (e.g. $\hat{p}(u_1, u_2, u_3) = \hat{f}_i(u_1 + 2u_2) + 2\hat{f}_i(u_3 + 3u_1) + c$), $\exists p \in \mathrm{Pol}(\mathbf{A}_{p_1,\ldots,p_n})$,

$$p(\bar{x}) = (0, \ldots, 0, \hat{p}(\bar{x}|_{L_{i+1}}), 0, \ldots, 0)$$

Computational problems over nilpotent algebras

> “...what matters about finite algebras is what they can compute.”
>
> — Joel VanderWerf’s PhD thesis

The equivalence problem for finite algebras

$\mathbf{A} = (A, f_1, \ldots, f_n)$... finite algebra

Circuit Equivalence Problem CEQV($\mathbf{A}$)

INPUT: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ circuits over $\mathbf{A}$

QUESTION: Does $\mathbf{A} \models p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$?

Circuit Satisfaction Problem CSAT($\mathbf{A}$)

INPUT: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ circuits over $\mathbf{A}$

QUESTION: Does $p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)$ have a solution in $\mathbf{A}$?

In general CEQV($\mathbf{A}$) $\in$ coNP, CSAT($\mathbf{A}$) $\in$ NP

Question

What is the complexity for nilpotent Maltsev algebras $\mathbf{A}$?

Note: We may assume $q = 0$, since $p \approx q$ iff $m(p, q, 0) \approx 0$.

Intermission: Why circuits?

Circuits over an algebra $\mathbf{A} = (A, f_1, \ldots, f_n)$ encode the polynomial / term operations over $\mathbf{A}$ - **and they are good at it!**

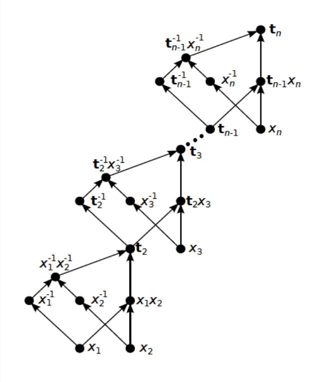
Example

In $(A_4, \cdot, ^{-1})$, the operations $t_n(x_1, \ldots, x_n) = [\cdots[[x_1, x_2], x_3], \ldots, x_n]$ with $[x, y] = x^{-1}y^{-1}xy$ has size $\mathcal{O}(2^n)$ as a term, but size $\mathcal{O}(n)$ as a circuit.

Encoding by circuits is

- more compact than encoding by terms
- size stable under polynomial equivalence

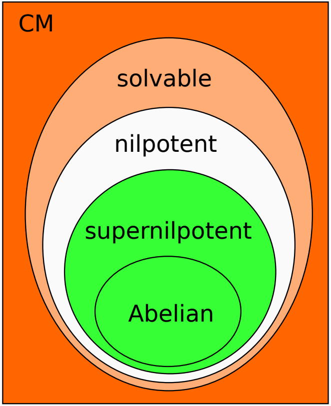
$\rightsquigarrow$ CEQV($\mathbf{A}$) $\leq$ CEQV($\mathbf{A}'$) if Pol($\mathbf{A}$) $\subseteq$ Pol($\mathbf{A}'$)



© Idziak, Krzaczkowski

CEQV **in congruence modular varieties**

A... from congruence modular variety:



- **A** Abelian $\leftrightarrow$ module. CEQV(**A**) $\in$ P
- **A** k-supernilpotent. CEQV(**A**) $\in$ P
  (Aichinger, Mudrinski '10)
- **A nilpotent, not supernilpotent...?**
- **A** solvable, non-nilpotent
  $\exists\theta$: CEQV($\mathbf{A}/\theta$) $\in$ coNP-c
  (Idziak, Krzaczkowski '18)
- **A** non-solvable: CEQV(**A**) $\in$ coNP-c
  (Idziak, Krzaczkowski '18)

For CSAT the picture is similar (modulo products with DL algebras).

It's all about the clonoids

Assume $\mathbf{A} \cong \mathbf{L} \otimes \mathbf{U}$, where $\mathbf{A}$ is n-nilpotent, and $\mathbf{U}$ is $(n-1)$-nilpotent. Every polynomial/circuit $p \in \mathrm{Pol}(\mathbf{A})$ can be represented as

$$p^{\mathbf{A}}((l_1, u_1), \ldots, (l_n, u_n)) = (p^{\mathbf{L}}(l_1, \ldots, l_n) + \hat{p}(u_1, \ldots, u_n), p^{\mathbf{U}}(u_1, \ldots, u_n))$$

Then $p^{\mathbf{A}}(x_1, \ldots, x_n) \approx 0$ iff

- $p^{\mathbf{U}}(u_1, \ldots, u_n) \approx 0$
- $p^{\mathbf{L}}(l_1, \ldots, l_n) \approx c$ and $\hat{p}(u_1, \ldots, u_n) \approx -c$ for some constant $c \in L$

Wishful thinking

By checking $\hat{p} \approx c$ somehow, we can reduce CEQV($\mathbf{A}$) to CEQV($\mathbf{U}$) in polynomial time. So CEQV($\mathbf{A}$) is in P.

Intermediate complexities for $\mathrm{CEQV}(\mathbf{A}_{p_1,\ldots,p_n})$

Polynomials over $\mathbf{A}_{p_1,\ldots,p_n}$

In $\mathbf{A}_{p_1,p_2} = \mathbb{Z}_{p_1} \otimes \mathbb{Z}_{p_2}$, with $p_1 \neq p_2$ there are polynomials $s_m((l_1, u_1), \ldots, (l_m, u_m)) = (\hat{s}_m(u_1, \ldots, u_m), 0)$ of size $\mathcal{O}(2^m)$ with

$$\hat{s}_m(u_1, \ldots, u_m) = \begin{cases} 0 \text{ if } \exists u_i = 0 \text{ else.} \\ 1 \text{ else.} \end{cases}.$$

Consequences

By composing such polynomials in $\mathbf{A}_{p_1,\ldots,p_n} = \mathbb{Z}_{p_1} \otimes \mathbb{Z}_{p_2} \otimes \cdots \otimes \mathbb{Z}_{p_n}$: $\exists t_m(x_1, \ldots, x_m) \in \mathrm{Pol}(\mathbf{A}_{p_1,\ldots,p_n})$, such that

- $t_m(x_1, \ldots, x_m) = (\hat{t}_m(x_1|_{\mathbb{Z}_{p_n}}, \ldots, x|_{\mathbb{Z}_{p_n}}), 0, \ldots, 0)$, with

$$\hat{t}_m(u_1, \ldots, u_m) = \begin{cases} 0 \text{ if } \exists u_i = 0 \\ 1 \text{ else.} \end{cases}$$

- $t_m(x_1, \ldots, x_m)$ has size $\mathcal{O}(2^{m^{1/d}})$ with $d = |\{i : p_i \neq p_{i+1}\}|$

A quasipolynomial lower bound using ETH

Exponential time hypothesis (ETH)

- The complexity of 3-SAT has a lower bound of $\mathcal{O}(c^n)$ for some $c > 1$
- The complexity of s-COLOR has a lower bound of $\mathcal{O}(c^n)$ for some $c > 1$

Theorem (Idziak, Kawałek, Krzaczkowski '20)
If ETH holds, then $\mathrm{CEQV}(\mathbf{A}_{p_1,\ldots,p_n})$ and $\mathrm{CSAT}(\mathbf{A}_{p_1,\ldots,p_n})$ have quasipolynomial lower bounds $\mathcal{O}(c^{\log(|p|)^d})$.

Pawel Idziak's ICALP talk:
`https://www.youtube.com/watch?v=0hWjHTE8hwI`

Proof sketch

We encode p_n-COLOR in CEQV($\mathbf{A}_{p_1,\dots,p_n}$):

- Let $G = (V, E)$ be an instance of p_n-COLOR
- Let $(v_1, w_1), \dots (v_{|E|}, w_{|E|})$ be enumeration of all edges
- Then take the equation in variables $(x_v)_{v \in V}$:

$$t_{|E|}(x_{v_1} - x_{w_1}, \dots, x_{v_{|E|}} - x_{w_{|E|}}) \approx 0$$

This equation has size $\mathcal{O}(c^{|E|^{1/d}})$, and only depends on values of $x_v|_{\mathbb{Z}_{p_n}}$.
It holds if and only if G is not p_n-colorable.

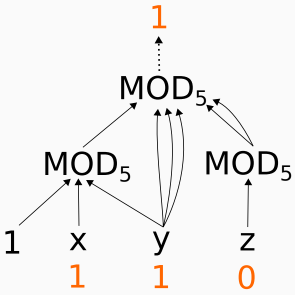
p_n-COLOR has lower bound $\mathcal{O}(c^{|G|}) \Rightarrow$ CEQV($\mathbf{A}_{p_1,\dots,p_n}$) has $\mathcal{O}(c^{\log(|p|)^d})$. $\square$

Question: *Are* there quasipolynomial algorithms?

CC-circuits

A $CC[m]$-**circuit** is a Boolean circuit, whose gates are MOD_m-gates, of arbitrary fan-in:

$$\mathrm{MOD}_m(x_1, \ldots, x_n) = \begin{cases} 1 \text{ if } \sum_i x_i \equiv 0 \mod m \\ 0 \text{ else.} \end{cases}$$



Conjecture (BST '90)

$\forall m, d$: $CC[m]$-circuits of depth d need size $\mathcal{O}(2^{n^c})$ to compute $\mathrm{AND}(x_1, \ldots, x_n)$.

BST Conjecture

$\forall m, d$: $CC[m]$-circuits of depth d need exponential size $\mathcal{O}(2^{n^c})$ to compute $\text{AND}(x_1, \dots, x_n)$

An operation $f : A^k \to A$ is called 0-**absorbing** iff $f(0, x_2, \dots, x_k) \approx f(x_1, 0, x_2, \dots, x_k) \approx \cdots \approx f(x_1, \dots, x_{k-1}, 0) \approx 0$.

If the BST conjecture holds for $m = p_1 \cdots p_n$ and depth $d = n$, then every non-constant 0-absorbing circuit $f(x_1, \dots, x_k)$ of $\mathbf{A}_{p_1,\dots,p_n}$ has size $\mathcal{O}(2^{k^c})$.

In fact BST implies (MK '19):

BST conjecture ('universal algebra version')

Let $\mathbf{A}$ be nilpotent, and $(p_k(x_1, \dots, x_k))_{k \in \mathbb{N}}$ be a sequence of non constant 0-absorbing polynomials. Then $|p_k| \geq \mathcal{O}(2^{k^c})$ (for some $c > 0$).

Quasipolynomial upper bounds

Theorem (MK '19)

Assume the BST conjecture holds for $\mathbf{A}$ nilpotent.

Then CEQV($\mathbf{A}$) and CSAT($\mathbf{A}$) can be solved in $\mathcal{O}(2^{\log(|p|)^c})$

Proof idea:

- Let $p(\bar{x}) \approx 0$ be an input to CEQV($\mathbf{A}$).
- Assume $\exists \bar{a} : p(\bar{a}) \neq 0$.
- Take $\bar{a}$ with minimal number k of $a_i \neq 0$, wlog. $\bar{a} = (a_1, \ldots, a_k, 0, \ldots, 0)$
- Then $p'(x_1, \ldots, x_k) = p(x_1, \ldots, x_k, 0, 0, \ldots, 0)$ is 0-absorbing.
- BST Conjecture $\Rightarrow k \leq \log(|p|)^c$
- To check $p(\bar{x}) \approx 0$, it is enough to evaluate p at all tuples with 'support' $\log(|p|)^c$ in time $\mathcal{O}(|p|^{\log(|p|)^c})$ $\square$

For $|A|$ is prime power: $k \leq \mathit{const}$

$\Rightarrow$ polynomial time algorithm for prime powers / supernilpotent.

(Aichinger, Mudrinski '10)

Summary

Summary

Assume that

- the *ETH* holds
- the *BST conjecture* hold, and
- $|\{i : p_i \neq p_{i+1}\}| \geq 2$.

Then CEQV($\mathbf{A}_{p_1,\ldots,p_n}$) and CSAT($\mathbf{A}_{p_1,\ldots,p_n}$) can be solved in quasipolynomial time $\mathcal{O}(2^{log(|p|)^c})$, but not in polynomial time!

CEQV($\mathbf{A}_{p_1,\ldots,p_n}$) is coNP-intermediate, and
CSAT($\mathbf{A}_{p_1,\ldots,p_n}$) is NP-intermediate

Questions

- How to obtain quasipolynomial lower bounds in general?
- How to then measure $|\{i : p_i \neq p_{i+1}\}|$?

How to deal with arbitrary nilpotent algebras?

The higher arity commutator

$\mathbf{A} = (A, (f^{\mathbf{A}})_{f \in \tau})$... algebra
$\alpha_1, \ldots, \alpha_n, \gamma \in \mathrm{Con}(\mathbf{A})$

- Then $C(\alpha_1, \ldots, \alpha_n; \gamma)$ if for all tuples $\bar{a}_i \, \alpha_i \, \bar{b}_i$

$$t(\bar{x}_1, \ldots, \bar{x}_{n-1}, \bar{a}_n) \, \gamma \, t(\bar{x}_1, \ldots, \bar{x}_n, \bar{b}_n),$$

  for all $(\bar{x}_1, \ldots, \bar{x}_{n-1}) \in \prod_{i=1}^{n-1} \{\bar{a}_i, \bar{b}_i\} \setminus \{(\bar{b}_1, \ldots, \bar{b}_{n-1})\}$ implies

$$t(\bar{b}_1, \ldots, \bar{b}_{n-1}, \bar{a}_n) \, \gamma \, t(\bar{b}_1, \ldots, \bar{b}_{n-1}, \bar{b}_n),$$

- The *higher commutator* $[\alpha_1, \ldots, \alpha_n]$ is the smallest γ with $C(\alpha_1, \ldots, \alpha_n; \gamma)$.

A congruence α is called *supernilpotent* if $[\alpha, \alpha, \ldots, \alpha] = 0_A$.

Fitting series

Let $\mathbf{A} \cong \mathbf{L}_1 \otimes \cdots \otimes \mathbf{L}_n$ corresponding to a maximal central series $0_A \prec \alpha_1 \prec \cdots \prec \alpha_n = 1_A$. Then

- Every $\mathbf{L}_j$ is a simple module (over $\mathbb{Z}_p^m$)
- α_i is supernilpotent, if and only if, there is no $p \in \mathrm{Pol}(\mathbf{A})$ such that $p|_{L_k}$ depends on coprime L_j, with $j < k \leq i$.

Definition

Let $\mathbf{A}$ be finite Maltsev algebra. Then

- $\exists$ *maximal* supernilpotent $\lambda \in \mathrm{Con}(\mathbf{A})$, the *Fitting congruence*.
- If $\mathbf{A}$ is nilpotent (solvable), the *(upper) Fitting series* is $0_A = \lambda_0 < \lambda_1 < \cdots < \lambda_l = 1_A$, such that $\lambda_i / \lambda_{i-1}$ is the Fitting congruence of $\mathbf{A}/\lambda_{i-1}$.
- $l :=$ *Fitting length* of $\mathbf{A}$.

Higher commutators and absorbing polynomials

Lemma (Aichinger, Mudrinski '10, MK '20)
Let **A** be a nilpotent Maltsev algebra, $0 \in A$, $\alpha_1, \ldots, \alpha_k \in \mathrm{Con}(\mathbf{A})$. Then $[\alpha_1, \ldots, \alpha_k]$ is generated by the pairs

$$\{(0, p(b_1, \ldots, b_k))\colon b_i \, \alpha_i \, 0 \text{ and } p \in \mathrm{Pol}(\mathbf{A}) \text{ is 0-absorbing}\}$$

The lemma allows us, e.g. to define an equivalence class of $[1_A, \ldots, 1_A]$ as the image of a polynomial.

Result

Theorem (...soon on arXiv?)
Let $\mathbf{A}$ be a finite nilpotent Maltsev algebra of Fitting length $l \geq 2$, and assume that ETH holds. Then CEQV($\mathbf{A}$) and CSAT($\mathbf{A}$) have lower bounds of $\mathcal{O}(2^{\log(|p|)^{l-1}})$.

Proof outline:

- Take $\mathbf{A} \cong \mathbf{L}_1 \otimes \cdots \otimes \mathbf{L}_n$, which corresponds to a maximal central series, extending the Fitting series
- find polynomials $t_m(x_1, \ldots, x_m)$ of size $\mathcal{O}(2^{m^{(l-1)^{-1}}})$, that only depend on L_n, map to L_1 an encode conjunctions
- This requires the previous lemmas and some patience (*)

Remark: Idziak et. al are proving it for finite *solvable* Maltsev algebras, using TCT.

Open questions

Question

What is the complexity of CEQV($\mathbf{A}$) and CSAT($\mathbf{A}$) of Fitting length 2?

Theorem (Kawałek, MK, Krzaczkowski '19)

For 2-nilpotent $\mathbf{A}$, CEQV($\mathbf{A}$) $\in$ P.

Question

How far can we generalize this tractability?

The end

Thank you!