SOME LESSONS ON COMPUTER ALGEBRA

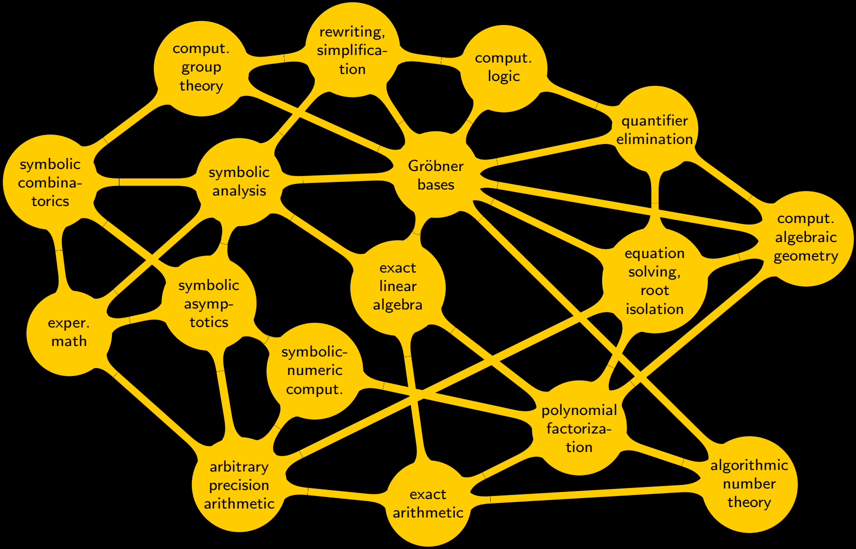
Manuel Kauers · Institute for Algebra · JKU

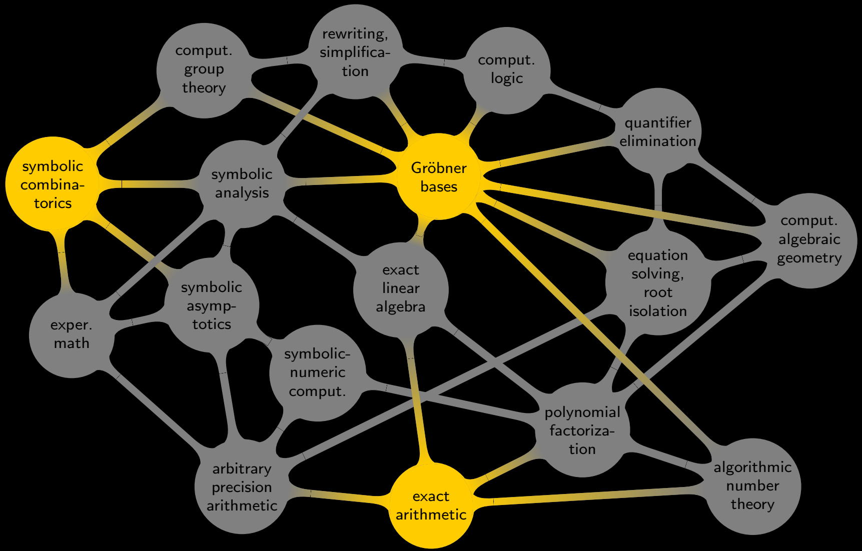
Slides available at https://tinyurl.com/y8h6l6sp

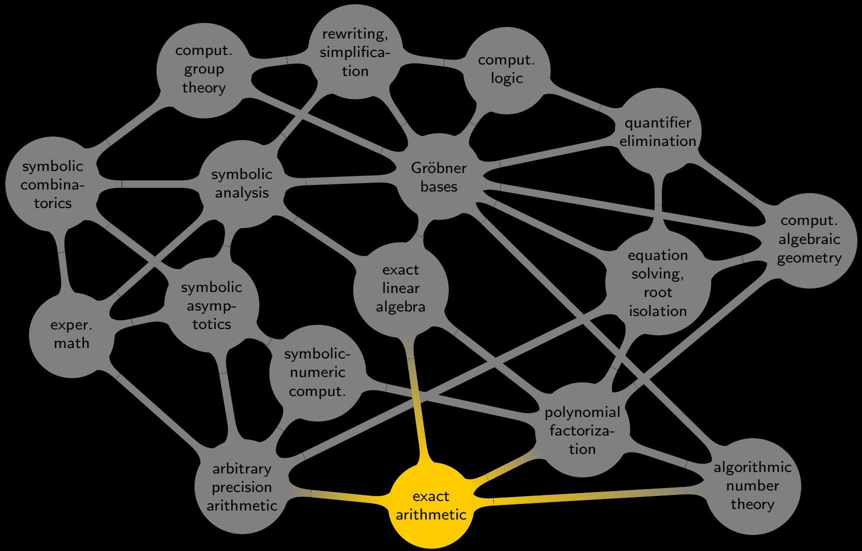
NINE LESSONS ON COMPUTER ALGEBRA

Manuel Kauers · Institute for Algebra · JKU

Slides available at https://tinyurl.com/y8h6l6sp


comput. group theory
rewriting, simplification
comput. logic
quantifier elimination
symbolic combinatorics
symbolic analysis
Gröbner bases
comput. algebraic geometry
exact linear algebra
equation solving, root isolation
exper. math
symbolic asymptotics
symbolic-numeric comput.
polynomial factorization
arbitrary precision arithmetic
exact arithmetic
algorithmic number theory


comput. group theory
rewriting, simplifica- tion
comput. logic
quantifier elimination
symbolic combina- torics
symbolic analysis
Gröbner bases
comput. algebraic geometry
equation solving, root isolation
exact linear algebra
symbolic asymp- totics
exper. math
symbolic- numeric comput.
polynomial factoriza- tion
arbitrary precision arithmetic
exact arithmetic
algorithmic number theory


comput. group theory
rewriting, simplification
comput. logic
quantifier elimination
symbolic combinatorics
symbolic analysis
Gröbner bases
comput. algebraic geometry
exact linear algebra
equation solving, root isolation
symbolic asymptotics
exper. math
symbolic-numeric comput.
polynomial factorization
arbitrary precision arithmetic
exact arithmetic
algorithmic number theory

$$+ \quad - \quad \times \quad \div \quad \mathrm{quo} \quad \mathrm{rem} \quad \mathrm{gcd} \quad \stackrel{?}{=}$$

$$+ \quad - \quad \times \quad \div \quad \mathsf{quo} \quad \mathsf{rem} \quad \mathsf{gcd} \quad \stackrel{?}{=}$$

$$2457234957927694576945792851 \in \mathbb{Z}$$

$$\frac{39376943576394575193475}{9763947613453694769351} \in \mathbb{Q}$$

$$2.718281828459045235360287471352662497\ldots \in \mathbb{R}$$

$$\bullet x^6 + \bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet \in k[x]$$

$$\frac{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet}{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet} \in k(x)$$

$$\bullet + \bullet x + \bullet x^2 + \bullet x^3 + \bullet x^4 + \bullet x^5 + \bullet x^6 + \cdots \in k[[x]]$$

$$+ \quad - \quad \times \quad \div \quad \text{quo} \quad \text{rem} \quad \text{gcd} \quad \stackrel{?}{=}$$

$$2457234957927694576945792851 \in \mathbb{Z} \qquad \checkmark$$

$$\frac{39376943576394575193475}{9763947613453694769351} \in \mathbb{Q}$$

$$2.718281828459045235360287471352662497\ldots \in \mathbb{R}$$

$$\bullet x^6 + \bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet \in k[x]$$

$$\frac{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet}{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet} \in k(x)$$

$$\bullet + \bullet x + \bullet x^2 + \bullet x^3 + \bullet x^4 + \bullet x^5 + \bullet x^6 + \cdots \in k[[x]]$$

$$+ \quad - \quad \times \quad \div \quad \text{quo} \quad \text{rem} \quad \text{gcd} \quad \stackrel{?}{=}$$

$$2457234957927694576945792851 \in \mathbb{Z} \qquad \checkmark$$

$$\frac{39376943576394575193475}{97639476134536947693 51} \in \mathbb{Q} \qquad \checkmark$$

$$2.7182818284590452353602874713526624977\ldots \in \mathbb{R}$$

$$\bullet x^6 + \bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet \in k[x]$$

$$\frac{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet}{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet} \in k(x)$$

$$\bullet + \bullet x + \bullet x^2 + \bullet x^3 + \bullet x^4 + \bullet x^5 + \bullet x^6 + \cdots \in k[[x]]$$

$$+ \quad - \quad \times \quad \div \quad \text{quo} \quad \text{rem} \quad \text{gcd} \quad \stackrel{?}{=}$$

$$2457234957927694576945792851 \in \mathbb{Z} \qquad \checkmark$$

$$\frac{39376943576394575193475}{9763947613453694769351} \in \mathbb{Q} \qquad \checkmark$$

$$2.718281828459045235360287471352662497\ldots \in \mathbb{R} \qquad \times$$

$$\bullet x^6 + \bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet \in k[x]$$

$$\frac{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet}{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet} \in k(x)$$

$$\bullet + \bullet x + \bullet x^2 + \bullet x^3 + \bullet x^4 + \bullet x^5 + \bullet x^6 + \cdots \in k[[x]]$$

$$+ \quad - \quad \times \quad \div \quad \text{quo} \quad \text{rem} \quad \text{gcd} \quad \stackrel{?}{=}$$

$$2457234957927694576945792851 \in \mathbb{Z} \qquad \checkmark$$

$$\frac{39376943576394575193475}{9763947613453694769351} \in \mathbb{Q} \qquad \checkmark$$

$$2.718281828459045235360287471352662497\ldots \in \mathbb{R} \qquad \times$$

$$\bullet x^6 + \bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet \in k[x] \qquad \checkmark$$

$$\frac{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet}{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet} \in k(x)$$

$$\bullet + \bullet x + \bullet x^2 + \bullet x^3 + \bullet x^4 + \bullet x^5 + \bullet x^6 + \cdots \in k[[x]]$$

$+ \quad - \quad \times \quad \div \quad \text{quo} \quad \text{rem} \quad \text{gcd} \quad \stackrel{?}{=}$

$$2457234957927694576945792851 \in \mathbb{Z} \qquad \checkmark$$

$$\frac{39376943576394575193475}{9763947613453694769351} \in \mathbb{Q} \qquad \checkmark$$

$$2.718281828459045235360287471352662497\ldots \in \mathbb{R} \qquad \times$$

$$\bullet x^6 + \bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet \in k[x] \qquad \checkmark$$

$$\frac{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet}{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet} \in k(x) \qquad \checkmark$$

$$\bullet + \bullet x + \bullet x^2 + \bullet x^3 + \bullet x^4 + \bullet x^5 + \bullet x^6 + \cdots \in k[[x]]$$

$$+ \quad - \quad \times \quad \div \quad \text{quo} \quad \text{rem} \quad \text{gcd} \quad \stackrel{?}{=}$$

$$2457234957927694576945792851 \in \mathbb{Z} \qquad \checkmark$$

$$\frac{39376943576394575193475}{9763947613453694769351} \in \mathbb{Q} \qquad \checkmark$$

$$2.718281828459045235360287471352662497\ldots \in \mathbb{R} \qquad \times$$

$$\bullet x^6 + \bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet \in k[x] \qquad \checkmark$$

$$\frac{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet}{\bullet x^5 + \bullet x^4 + \bullet x^3 + \bullet x^2 + \bullet x + \bullet} \in k(x) \qquad \checkmark$$

$$\bullet + \bullet x + \bullet x^2 + \bullet x^3 + \bullet x^4 + \bullet x^5 + \bullet x^6 + \cdots \in k[[x]] \qquad \sim$$

$$\begin{array}{r} 314744866848 \times 8246147938 76 \\ \hline \\ \\ \\ \hline \end{array}$$

$$31474486848 \times 824614793876$$

Computation time grows quadratically with the input size.

Computation time grows quadratically with the input size.

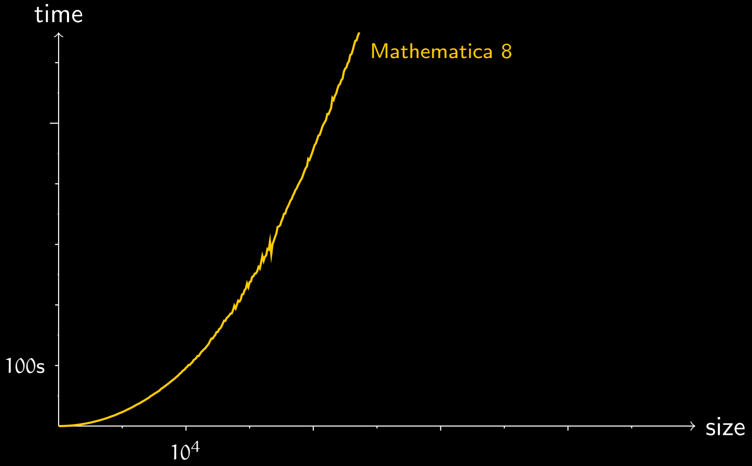
Modern algorithms have (quasi-)linear computation time.

Computation time grows quadratically with the input size.

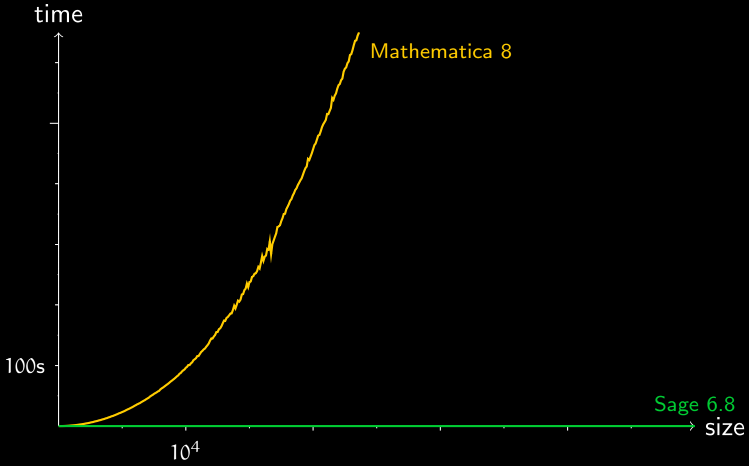
Modern algorithms have (quasi-)linear computation time.

For which input sizes does the difference matter?

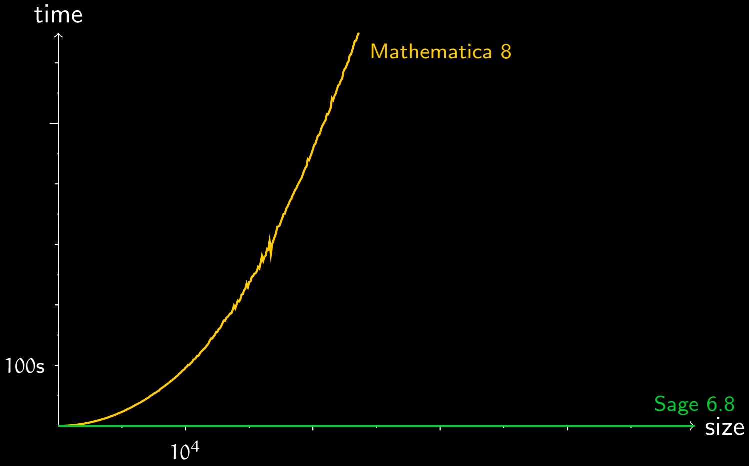
Polynomial Multiplication



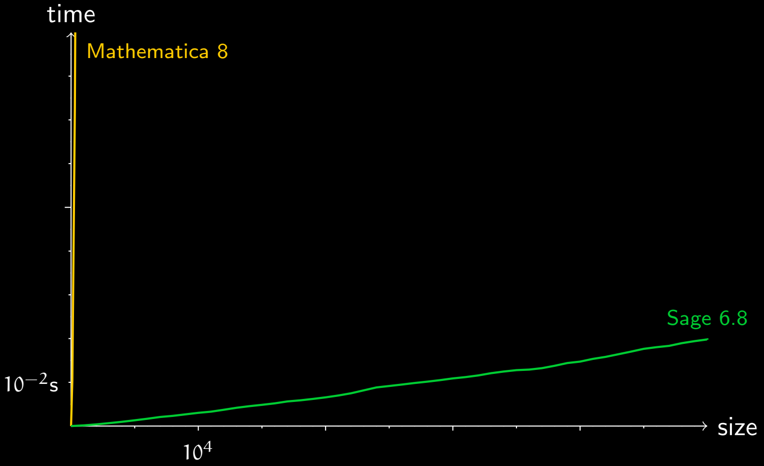
Polynomial Multiplication



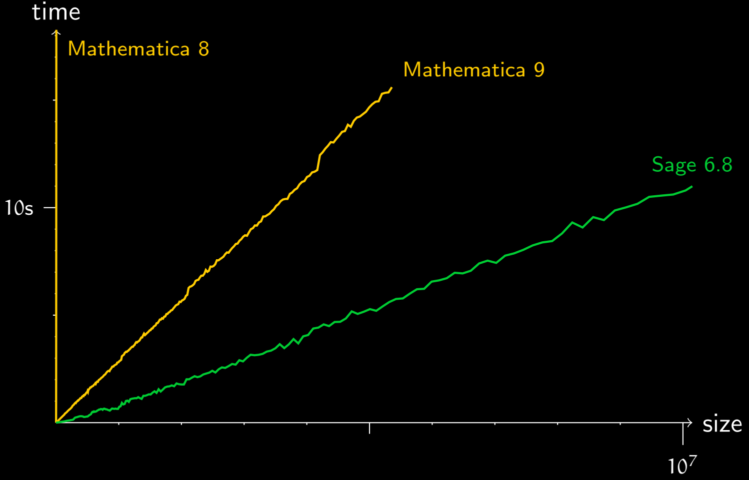
Polynomial Multiplication



Polynomial Multiplication



Polynomial Multiplication



Lesson 1: Fast algorithms are really fast

Fast multiplication has no advantage if the input is too unbalanced.

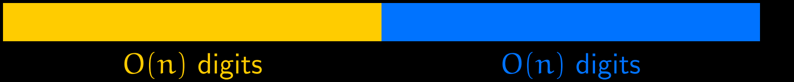
Fast multiplication has no advantage if the input is too unbalanced.

good input:

$O(n)$ digits $O(n)$ digits

Fast multiplication has no advantage if the input is too unbalanced.

good input:



not so good input (naive multiplication also takes linear time):

Example: computing $n!$ for large n.

Example: computing $n!$ for large n.

Naive:

$$8! = \boxed{\boxed{\boxed{\boxed{\boxed{\boxed{\boxed{1 \cdot 2} \cdot 3} \cdot 4} \cdot 5} \cdot 6} \cdot 7} \cdot 8}$$

$T(n) = \sum_{k=1}^{n} O(k) = O(n^2)$, even with fast multiplication.

Example: computing $n!$ for large n.

Naive:

$$8! = \boxed{\boxed{\boxed{\boxed{\boxed{\boxed{\boxed{1 \cdot 2} \cdot 3} \cdot 4} \cdot 5} \cdot 6} \cdot 7} \cdot 8}$$

$T(n) = \sum_{k=1}^{n} O(k) = O(n^2)$, even with fast multiplication.

Balanced:

$$8! = \boxed{\boxed{\boxed{1 \cdot 2} \cdot \boxed{3 \cdot 4}} \cdot \boxed{\boxed{5 \cdot 6} \cdot \boxed{7 \cdot 8}}}$$

$T(n) = 2T(n/2) + \tilde{O}(n) \Rightarrow T(n) = \tilde{O}(n)$ with fast multiplication.

Take this into account when you need to compute terms of large index of a P-recursive sequence.

$$p_0(n)a_n + p_1(n)a_{n+1} + p_2(n)a_{n+2} = 0$$

Take this into account when you need to compute terms of large index of a P-recursive sequence.

$$\begin{pmatrix} a_{n+1} \\ a_{n+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -\frac{p_0(n)}{p_2(n)} & -\frac{p_1(n)}{p_2(n)} \end{pmatrix} \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix}$$

Take this into account when you need to compute terms of large index of a P-recursive sequence.

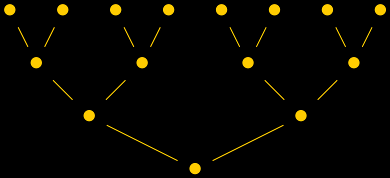
$$\begin{pmatrix} a_{n+1} \\ a_{n+2} \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \\ -\frac{p_0(n)}{p_2(n)} & -\frac{p_1(n)}{p_2(n)} \end{pmatrix}}_{=:C(n)} \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix}$$

Take this into account when you need to compute terms of large index of a P-recursive sequence.

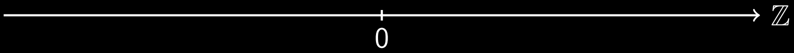
$$\begin{pmatrix} a_{n+1} \\ a_{n+2} \end{pmatrix} = C(n-2)C(n-3)C(n-4)\cdots C(2)\begin{pmatrix} a_0 \\ a_1 \end{pmatrix}.$$

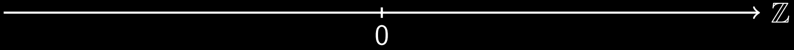
Take this into account when you need to compute terms of large index of a P-recursive sequence.

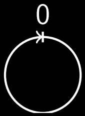
$$\begin{pmatrix} a_{n+1} \\ a_{n+2} \end{pmatrix} = C(n-2)C(n-3)C(n-4)\cdots C(2) \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}.$$



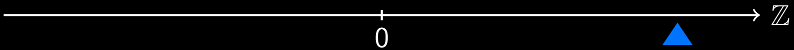
Lesson 2: Organize your computations well

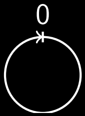

0
ℤ



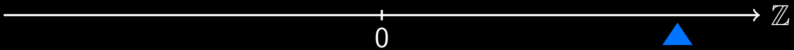


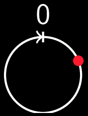
$$\mathbb{Z}_{1091} = \mathbb{Z}/1091\mathbb{Z}$$



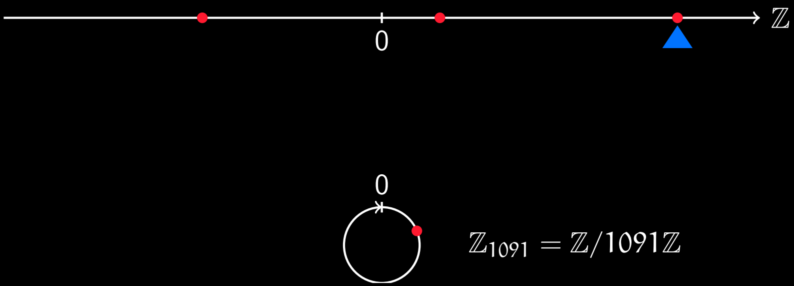


$$\mathbb{Z}_{1091} = \mathbb{Z}/1091\mathbb{Z}$$

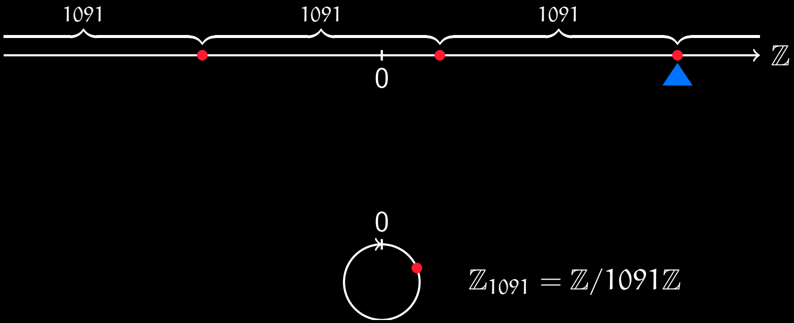




$$\mathbb{Z}_{1091} = \mathbb{Z}/1091\mathbb{Z}$$



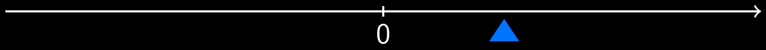
$$\mathbb{Z}_{1091} = \mathbb{Z}/1091\mathbb{Z}$$



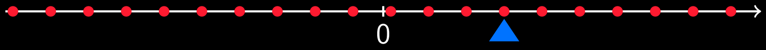
$$\mathbb{Z}_{1091} = \mathbb{Z}/1091\mathbb{Z}$$

For fixed $m \in \mathbb{Z} \setminus \{0\}$, let $f_m \colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $x \mapsto [x]_m := x + m\mathbb{Z}$.

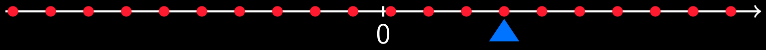
For fixed $m \in \mathbb{Z} \setminus \{0\}$, let $f_m\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $x \mapsto [x]_m := x + m\mathbb{Z}$.



For fixed $m \in \mathbb{Z} \setminus \{0\}$, let $f_m \colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $x \mapsto [x]_m := x + m\mathbb{Z}$.



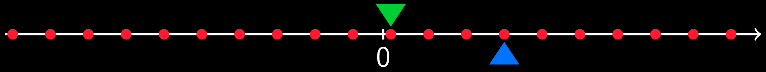
For fixed $m \in \mathbb{Z} \setminus \{0\}$, let $f_m \colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $x \mapsto [x]_m := x + m\mathbb{Z}$.



f_m is a ring homomorphism. This means

$$\text{Mod}(\text{Answer}(\text{Question})) = \text{Answer}(\text{Mod}(\text{Question}))$$

For fixed $m \in \mathbb{Z} \setminus \{0\}$, let $f_m \colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $x \mapsto [x]_m := x + m\mathbb{Z}$.

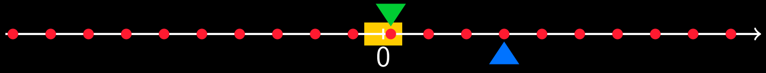


f_m is a ring homomorphism. This means

$$\text{Mod}(\text{Answer}(\text{Question})) = \text{Answer}(\text{Mod}(\text{Question}))$$

Represent $[x]_m$ by an element $\xi \in [x]_m$ for which $|\xi|$ is minimal.

For fixed $m \in \mathbb{Z} \setminus \{0\}$, let $f_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $x \mapsto [x]_m := x + m\mathbb{Z}$.



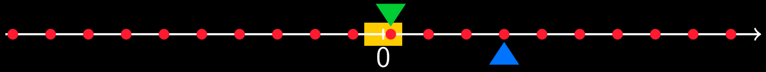
f_m is a ring homomorphism. This means

$$\text{Mod}(\text{Answer}(\text{Question})) = \text{Answer}(\text{Mod}(\text{Question}))$$

Represent $[x]_m$ by an element $\xi \in [x]_m$ for which $|\xi|$ is minimal.

- $\xi \in [-m/2, m/2]$.

For fixed $m \in \mathbb{Z} \setminus \{0\}$, let $f_m \colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $x \mapsto [x]_m := x + m\mathbb{Z}$.



f_m is a ring homomorphism. This means

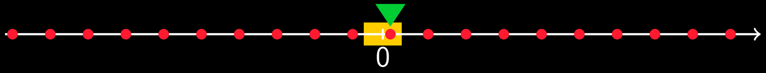
$$\text{Mod}(\text{Answer}(\text{Question})) = \text{Answer}(\text{Mod}(\text{Question}))$$

Represent $[x]_m$ by an element $\xi \in [x]_m$ for which $|\xi|$ is minimal.

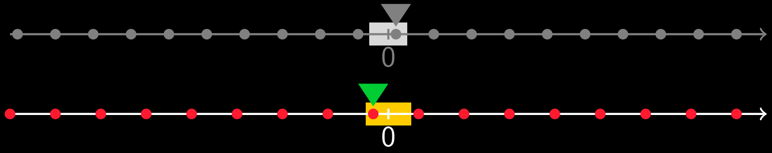
- $\xi \in [-m/2, m/2]$.
- If $m > 2|x|$ then $\xi = x$.

$x \in [x]_m$

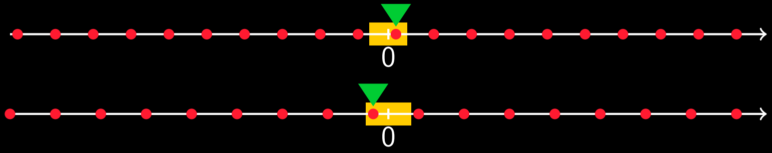
$x \in [x]_m$



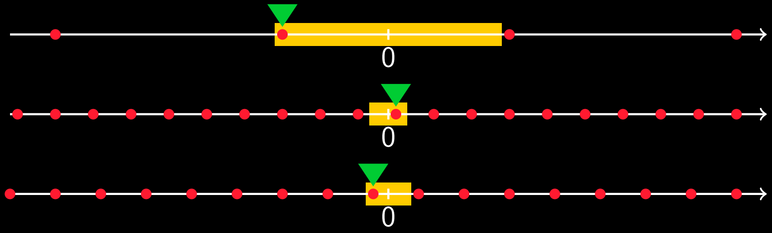
$x \in \qquad [x]_n$



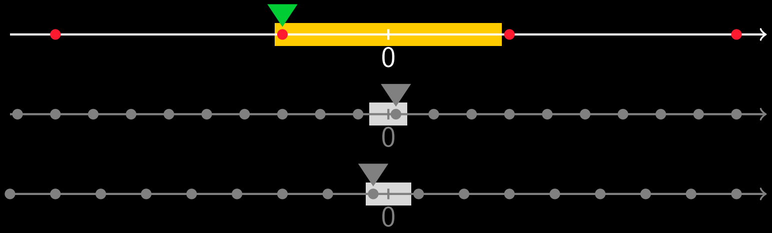
$x \in [x]_m \cap [x]_n$



$x \in [x]_m \cap [x]_n$

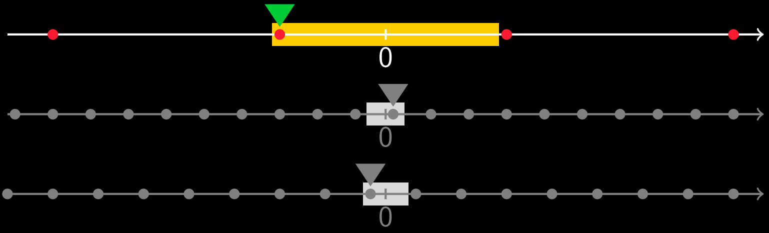


$$x \in [x]_m \cap [x]_n = [x]_{\mathrm{lcm}(m,n)}$$



Chinese Remaindering

$$x \in [x]_m \cap [x]_n = [x]_{\mathrm{lcm}(m,n)}$$



Chinese Remaindering

$$x \in [x]_m \cap [x]_n = [x]_{\mathsf{lcm}(m,n)}$$

Features:

Chinese Remaindering

$$x \in [x]_m \cap [x]_n = [x]_{\mathrm{lcm}(m,n)}$$

Features:

- Even a big integer x can be recovered from sufficiently many images $[x]_{m_1}, [x]_{m_2}, \ldots$ for small moduli $m_1, m_2, \ldots$.

Chinese Remaindering

$$x \in [x]_m \cap [x]_n = [x]_{\mathsf{lcm}(m,n)}$$

Features:

- Even a big integer x can be recovered from sufficiently many images $[x]_{m_1}, [x]_{m_2}, \ldots$ for small moduli $m_1, m_2, \ldots$.
- Different modular images $[x]_{m_i}$ can be computed in parallel on different computers.

0
170
57125
48268101
34260690332
28950283288564
24602777889341700
21958748103044947821
19982460773770890734814
18589778412414172744395308
17556405435959384905586216420
16804193264871415986848637912866
16258906633984352510780895055898688
15878645003134966488517342432611820340
15631047178991661938104976711572278528840
15494275516175484896146558165069374931768650
15452119731275448721521690374123048169473745090
15492944429910290948927453354128640277129701928270
15608195638318139575397871729737310479957231181434400
15791696434663015062086294548870131152897244600962599710
16039042304161558566190267565720083550110055872936313121300
16347221676787084843566201114528305144441011394615536628043480
16714327636344626391862041955812314792830121148741093212135914440
17139356963672793388669217006249699836555901801582671305065963412450
17622061542861347959625369356680682135593177881983900768539311826713472
18162841216793283422562091421291078521630723657702122424507756283808698700
18762665614999822007839830386311098144372506555360938018652662698220539694616
19423018217659251266276892430699632002229719351100435132025989366139940897600008
20145857126504814155109603745644558012097546254998545662831506345299150654223844360
20933588899934099785719806412698545336726130412328111385454392939736508704575356754888
21789052707980917749010589339181187870108450716708413481060716254608148803460083665644160

mod 18446744073709551557
0
170
57125
48268101
34260690332
28950283288564
24602777889341700
21958748103044947821
19982460773770890734814
18589778412414172744395308
17556405435959384905586216420
16804193264871415986848637912866
16258906633984352510780895055898688
15878645003134966488517342432611820340
15631047178991661938104976711572278528840
15494275516175484896146558165069374931768650
15452119731275448721521690374123048169473745090
15492944429910290948927453354128640277129701928270
15608195638318139575397871729737310479957231181434400
15791696434663015062086294548870131152897244600962599710
16039042304161558566190267565720083550110055872936313121300
16347221676787084843566201114528305144441011394615536628043480
16714327636344626391862041955812314792830121148741093212135914440
17139356963672793388669217006249699836555901801582671305065963412450
17622061542861347959625369356680682135593177881983900768539311826713472
18162841216793283422562091421291078521630723657702122424507756283808698700
18762665614999822007839830386311098144372506555360938018652662698220539694616
19423018217659251266276892430699632002229719351100435132025989366139940897600008
20145857126504814155109603745644558012097546254998545662831506345299150654223844360
20933588899934099785719806412698545336726130412328111385454392939736508704575356754888
21789052707980917749010589339181187870108450716708413481060716254608148803460083665644160

mod 18446744073709551557

0
170
57125
48268101
34260690332
28950283288564
24602777889341700
3512004029335396264
4636941943446398583
16731901151034173887
13561571021375624155
18327681355361409199
14135275161253345008
5637819232275028612
6637602357189385604
12482169677218181673
13064253343726879423
14625225362239686504
10738834608406986658
961106949064586405
2211804365157896289
8829591048746708080
15009988290858134393
7627367407386026140
14734287943773226198
15483359934879899009
899837740350271794
6952192533371026338
17697300886138518812
14174304902082598370
9566720042687775664

mod	18446744073709551557	18446744073709551533
	0	0
	170	170
	57125	57125
	48268101	48268101
	34260690332	34260690332
	28950283288564	28950283288564
	24602777889341700	24602777889341700
	3512004029335396264	3512004029335396288
	4636941943446398583	4636941943446424575
	16731901151034173887	16731901151058359959
	13561571021375624155	13561571044217255635
	18327681355361409199	18327703218332822743
	14135275161253345008	14156428691527110768
	5637819232275028612	7849868848795513175
	6637602357189385604	14984004752674089390
	12482169677218181673	12488827142696955539
	13064253343726879423	15658485480684595156
	14625225362239686504	10758223940600306782
	10738834608406986658	788602827186764443
	961106949064586405	12251039281660517429
	2211804365157896289	15185001070958618575
	8829591048746708080	10856515003962139665
	15009988290858134393	12838284889333222403
	7627367407386026140	8420246272424470758
	14734287943773226198	16693159135573847818
	15483359934879899009	16119877770365982383
	899837740350271794	11946950024840031118
	6952192533371026338	13765592352507043696
	17697300886138518812	7652266267821078126
	14174304902082598370	11862232204708398073
	9566720042687775664	6633630390749590552

mod	18446744073709551557	18446744073709551533	18446744073709551521
	0	0	0
	170	170	170
	57125	57125	57125
	48268101	48268101	48268101
	34260690332	34260690332	34260690332
	28950283288564	28950283288564	28950283288564
	24602777889341700	24602777889341700	24602777889341700
	3512004029335396264	3512004029335396288	3512004029335396300
	4636941943446398583	4636941943446424575	4636941943446437571
	16731901151034173887	16731901151058359959	16731901151070452995
	13561571021375624155	13561571044217255635	13561571055638071375
	18327681355361409199	18327703218332822743	18327714149818529515
	14135275161253345008	14156428691527110768	14167005456663993648
	5637819232275028612	7849868848795513175	18179265693910531235
	6637602357189385604	14984004752674089390	7104618767069095598
	12482169677218181673	12488827142696955539	12492155875456012980
	13064253343726879423	15658485480684595156	7732229531925667068
	14625225362239686504	10758223940600306782	8824742898598764285
	10738834608406986658	788602827186764443	5056674106894750910
	961106949064586405	12251039281660517429	1050611245293959755
	2211804365157896289	15185001070958618575	127308807730230649
	8829591048746708080	10856515003962139665	11318493766728410726
	15009988290858134393	12838284889333222403	8119518874668080973
	7627367407386026140	8420246272424470758	13169248223630974435
	14734287943773226198	16693159135573847818	2788562657830915054
	15483359934879899009	16119877770365982383	2471600991651671889
	899837740350271794	11946950024840031118	14756123186994554460
	6952192533371026338	13765592352507043696	11362094742791890224
	17697300886138518812	7652266267821078126	16010169456545623593
	14174304902082598370	11862232204708398073	1837996549587781514
	956672004268775664	6633630390749590552	1873712421652022656

mod	18446744073709551557	18446744073709551533	18446744073709551521	18446744073709551437
	0	0	0	0
	170	170	170	170
	57125	57125	57125	57125
	48268101	48268101	48268101	48268101
	34260690332	34260690332	34260690332	34260690332
	28950283288564	28950283288564	28950283288564	28950283288564
	24602777889341700	24602777889341700	24602777889341700	24602777889341700
	3512004029335396264	3512004029335396288	3512004029335396300	3512004029335396384
	4636941943446398583	4636941943446424575	4636941943446437571	4636941943446528543
	16731901151034173887	16731901151058359959	16731901151070452995	16731901151155104247
	13561571021375624155	13561571044217255635	13561571055638071375	13561571135583781555
	18327681355361409199	18327703218332822743	18327714149818529515	18327790670218476919
	14135275161253345008	14156428691527110768	14167005456663993648	14241042812622173808
	5637819232275028612	7849868848795513175	18179265693910531235	16698067314877451907
	6637602357189385604	14984004752674089390	710461876706909598	11476126187194330620
	12482169677218181673	12488827142696955539	12492155875456012980	12515457005136597883
	13064253343726879423	15658485480684595156	7732229531925667068	7588670477925634811
	14625225362239686504	10758223940600306782	8824742898598764285	13737486829569602371
	10738834608406986658	788602827186764443	5056674106894750910	16856311482456444934
	961106949064586405	12251039281660517429	1050611245293959755	1730796780127391701
	2211804365157896289	15185001070958618575	127308807730230649	2923290836694930836
	8829591048746708080	10856515003962139665	11318493766728410726	16555821147378467083
	15009988290858134393	12838284889333222403	8119518874668080973	11805308573535485946
	7627367407386026140	8420246272424470758	13169248223630974435	16982273330702579648
	14734287943773226198	16693159135573847818	2788562657830915054	17719370099115195915
	15483359934879899009	16119877770365982383	2471600991651671889	5095243575810575316
	899837740350271794	11946950024840031118	14756123186994554460	11226634917845487051
	6952192533371026338	13765592352507043696	11362094742791890224	6644727374610071491
	17697300886138518812	7652266267821078126	16010169456545623593	5224069660619876239
	14174304902082598370	11862232204708398073	1837996549587781514	1149810384458158270
	9566720042687775664	6633630390749590552	1873712421652022656	15580979477818358327

mod	18446744073709551557	18446744073709551533	18446744073709551521	18446744073709551437	18446744073709551427
	0	0	0	0	0
	170	170	170	170	170
	57125	57125	57125	57125	57125
	48268101	48268101	48268101	48268101	48268101
	34260690332	34260690332	34260690332	34260690332	34260690332
	28950283288564	28950283288564	28950283288564	28950283288564	28950283288564
	24602777889341700	24602777889341700	24602777889341700	24602777889341700	24602777889341700
	3512004029335396264	3512004029335396288	3512004029335396300	3512004029335396384	3512004029335396394
	4636941943446398583	4636941943446424575	4636941943446437571	4636941943446528543	4636941943446539373
	16731901151034173887	16731901151058359959	16731901151070452995	16731901151155104247	16731901151165181777
	13561571021375624155	13561571044217255635	13561571055638071375	13561571135583781555	13561571145101128005
	18327681355361409199	18327703218332822743	18327714149818529515	18327790670218476919	18327799779789899229
	14135275161253345008	14156428691527110768	14167005456663993648	14241042812622173808	14249856783569576208
	5637819232275028612	7849868848795513175	18179265693910531235	16698067314877451907	6859153945430415570
	6637602357189385604	14984004752674089390	710461876706909598	11476126187194330620	18028251197597986227
	12482169677218181673	12488827142696955539	12492155875456012980	12515457005136597883	9443773603570734321
	13064253343726879423	15658485480684595156	7732229531925667068	7588670477925634811	13281286656044656459
	14625225362239686504	10758223940600306782	8824742898598764285	13737486829569602371	15200796479896019943
	10738834608406986658	788602827186764443	5056674106894750910	16856311482456444934	17425730095808525587
	961106949064586405	12251039281660517429	1050611245293959755	1730796780127391701	635703020769662299
	2211804365157896289	15185001070958618575	127308807730230649	2923290836694930836	5446680587098832013
	8829591048746708080	10856515003962139665	11318493766728410726	16555821147378467083	2644477152643434420
	15009988290858134393	12838284889333222403	8119518874668080973	11805308573535485946	12562094561654048160
	7627367407386026140	8420246272424470758	13169248223630974435	16982273330702579648	6264853543132966636
	14734287943773226198	16693159135573847818	2788562657830915054	17719370099115195915	14351987686736218119
	15483359934879899009	16119877770365982383	2471600991651671889	5095243575810575316	12472610336651567052
	899837740350271794	11946950024840031118	14756123186994554460	11226634917845487051	13567859892950511514
	6952192533371026338	13765592352507043696	11362094742791890224	6644727374610071491	3992711139584800062
	17697300886138518812	7652266267821078126	16010169456545623593	5224069660619876239	13020528712638715163
	14174304902082598370	11862232204708398073	1837996549587781514	1149810384458158270	6569058788386309488
	9566720042687775664	6633630390749590552	1873712421652022656	15580979477818358327	7459210887944253892

https://tinyurl.com/y8h6l6sp

mod	340282366920938460843936948965011886881	18446744073709551521	18446744073709551437	18446744073709551427
	0	0	0	0
	170	170	170	170
	57125	57125	57125	57125
	48268101	48268101	48268101	48268101
	34260690332	34260690332	34260690332	34260690332
	28950283288564	28950283288564	28950283288564	28950283288564
	24602777889341700	24602777889341700	24602777889341700	24602777889341700
	21958748103044947821	3512004029335396300	3512004029335396384	3512004029335396394
	19982460773770890734814	4636941943446437571	4636941943446528543	4636941943446539373
	18589778412414172744395308	16731901151070452995	16731901151155104247	16731901151165181777
	17556405435959384905586216420	13561571055638071375	13561571135583781555	13561571145101128005
	16804193264871415986848637912866	18327714149818529515	18327790670218476919	18327799779789899229
	16258906633984352510780895055898688	14167005456663993648	14241042812622173808	14249856783569576208
	15878645003134966488517342432611820340	18179265693910531235	16698067314877451907	6859153945430415570
	318340667549431200127814008146743619195	7104618767069095 98	11476126187194330620	18028251197597986227
	198503164393958539577067845488686416077	12492155875456012980	12515457005136597883	9443773603570734321
	214670443338013688390580445819797373152	7732229531925667068	7588670477925634811	13281286656044656459
	138812086818822165420022065635983834073	8824742898598764285	13737486829569602371	15200796479896019943
	34887405067523117228515541823719337570	5056674106894750910	16856311482456444934	17425730095808525587
	86776038478706601837072280099789115 87	1050611245293959755	1730796780127391701	6357030207696622 99
	151755704527465931623446269946736011627	127308807730230649	2923290836694930836	5446680587098832013
	157520674316210552357179003218400644894	11318493766728410726	16555821147378467083	2644477152643434420
	83401389361404009186691170000994753262	8119518874668080973	11805308573535485946	12562094561654048160
	199107465433248163983566865568541300580	13169248223630974435	16982273330702579648	6264853543132966636
	171646799941657083902142563883114122236	2788562657830915054	17719370099115195915	14351987686736218119
	255701011924435651472375478434132710558	2471600991651671889	5095243575810575316	12472610336651567052
	65204696697886220698264621831639730752	14756123186994554460	11226634917845487051	13567859892950511514
	147021196331035236134827717045673809472	11362094742791890224	6644727374610071491	3992711139584800062
	304204745393541316784616770985857479782	16010169456545623593	5224069660619876239	13020528712638715163
	69115067553184129907739559131736482619	1837996549587781514	1149810384458158270	6569058788386309488
	338027952164498897207398828653950753404	1873712421652022656	15580979477818358327	7459210887944253892

mod	6277101735386680683188868462945250914462856766432493496001	18446744073709551437	18446744073709551427
	0	0	0
	170	170	170
	57125	57125	57125
	48268101	48268101	48268101
	34260690332	34260690332	34260690332
	28950283288564	28950283288564	28950283288564
	24602777889341700	24602777889341700	24602777889341700
	21958748103044947821	3512004029335396384	3512004029335396394
	19982460773770890734814	4636941943446528543	4636941943446539373
	18589778412414172744395308	16731901151155104247	16731901151165181777
	17556405435959384905586216420	13561571135583781555	13561571145101128005
	16804193264871415986848637912866	18327790670218476919	18327799779789899229
	16258906633984352510780895055898688	14241042812622173808	14249856783569576208
	15878645003134966488517342432611820340	16698067314877451907	6859153945430415570
	15631047178991661938104976711572278528840	11476126187194330620	18028251197597986227
	15494275516175484896146558165069374931768650	12515457005136597883	9443773603570734321
	15452119731275448721521690374123048169473745090	7588670477925634811	13281286656044656459
	15492944429910290948927453354128640277129701928270	13737486829569602371	15200796479896019943
	15608195638318139575397871729737310479957231181434400	16856311482456444934	17425730095808525587
	15791696434663015062086294548870131152897244600962599710	1730796780127391701	635703020769662299
	3484838833388197199812530639829581721184342340071326129298	2923290836694930836	5446680587098832013
	1648757840168344542387637018871763179732374825323564456876	16555821147378467083	2644477152643434420
	98850683949423615211578699701347807145350036885633235694	11805308573535485946	12562094561654048160
	526520284143404569767963343550807344171168366801172331356	16982273330702579648	6264853543132966636
	424185829625587809592566352271431402775173490353367407331	17719370099115195915	14351987686736218119
	4536991382758228630399221995435899884055743908863240725052	5095243575810575316	12472610336651567052
	3136412773560944376264550097061623603163416527516137221129	11226634917845487051	13567859892950511514
	5967388207129134077295313527201750659161648724805358750622	6644727374610071491	3992711139584800062
	853298661596862590652819419782007714434001836607900281638	5224069660619876239	13020528712638715163
	58401078608611669601836308424511522173492016757242657971	1149810384458158270	6569058788386309488
	1566681274568203485091061424628061282383374029659900022897	15580979477818358327	7459210887944253892

mod	115792089237316192812296663087828730790152317073519228853714845075653663303437	18446744073709551427
	0	0
	170	170
	57125	57125
	48268101	48268101
	34260690332	34260690332
	28950283288564	28950283288564
	24602777889341700	24602777889341700
	21958748103044947821	3512004029335396394
	19982460773770890734814	4636941943446539373
	18589778412414172744395308	16731901151165181777
	17556405435959384905586216420	13561571145101128005
	16804193264871415986848637912866	18327799779789899229
	16258906633984352510780895055898688	14249856783569576208
	15878645003134966488517342432611820340	6859153945430415570
	15631047178991661938104976711572278528840	18028251197597986227
	15494275516175484896146558165069374931768650	9443773603570734321
	15452119731275448721521690374123048169473745090	13281286656044656459
	15492944429910290948927453354128640277129701928270	15200796479896019943
	15608195638318139575397871729737310479957231181434400	17425730095808525587
	15791696434663015062086294548870131152897244600962599710	6357030207696662299
	16039042304161558566190267565720083550110055872936313121300	5446680587098832013
	16347221676787084843566201114528305144441011394615536628043480	2644477152643434420
	16714327636344626391862041955812314792830121148741093212135914440	12562094561654048160
	17139356963672793388669217006249699836555901801582671305065963412450	6264853543132966636
	17622061542861347959625369356680682135593177881983900768539311826713472	14351987686736218119
	18162841216793283422562091421291078521630723657702122424507756283808698700	12472610336651567052
	18762665614999822007839830386311098144372506555360938018652662698220539694616	13567859892950511514
	85739315027447066623349695032233960274282399822723913455610238505779125926029	3992711139584800062
	20647288309810477934116348519430344756735964496691756364545016993517019647 89	13020528712638715163
	23492476077323556255109014236440192037570229930868243250459695379292868666014	6569058788386309488
	11119080898386295262036368572079052970778552473889843769222187647716672660 6643	7459210887944253892

mod 2135987035920910012340807717593254758583661964006908954235666935176520392717928060033632257354599
0
170
57125
48268101
34260690332
28950283288564
24602777889341700
21958748103044947821
19982460773770890734814
18589778412414172744395308
17556405435959384905586216420
16804193264871415986848637912866
16258906633984352510780895055898688
15878645003134966488517342432611820340
15631047178991661938104976711572278528840
15494275516175484896146558165069374931768650
15452119731275448721521690374123048169473745090
15492944429910290948927453354128640277129701928270
15608195638318139575397871729737310479957231181434400
15791696434663015062086294548870131152897244600962599710
16039042304161558566190267565720083550110055872936313121300
16347221676787084843566201114528305144441011394615536628043480
16714327636344626391862041955812314792830121148741093212135914440
17139356963672793388669217006249699836555901801582671305065963412450
17622061542861347959625369356680682135593177881983900768539311826713472
18162841216793283422562091421291078521630723657702122424507756283808698700
18762665614999822007839830386311098144372506555360938018652662698220539694616
19423018217659251266276892430699632002229719351100435132025989366139940897600008
20145857126504814155109603745644558012097546254998545662831506345299150654223844360
20933588899934099785719806412698545336726130412328111385454392939736508704575356754888
21789052707980917749010589339181187870108450716708413481060716254608148803460083665644160

For hardware reasons, it's best to take primes of size $\approx 2^{64}$ or $\approx 2^{32}$ as moduli.

For hardware reasons, it's best to take primes of size $\approx 2^{64}$ or $\approx 2^{32}$ as moduli.

The number of moduli needed is then proportional to the length of the numbers in the final result.

For hardware reasons, it's best to take primes of size $\approx 2^{64}$ or $\approx 2^{32}$ as moduli.

The number of moduli needed is then proportional to the length of the numbers in the final result.

Significant saving happens only when the numbers in intermediate expressions are much longer.

For hardware reasons, it's best to take primes of size $\approx 2^{64}$ or $\approx 2^{32}$ as moduli.

The number of moduli needed is then proportional to the length of the numbers in the final result.

Significant saving happens only when the numbers in intermediate expressions are much longer.

Such intermediate expression swell is a common phenomenon in many calculations.

For example, the numbers on the previous slide satisfy a recurrence of order 4 and degree 10.

For example, the numbers on the previous slide satisfy a recurrence of order 4 and degree 10.

Around 60 terms are needed to recover it. The 60th term has 180 decimal digits.

For example, the numbers on the previous slide satisfy a recurrence of order 4 and degree 10.

Around 60 terms are needed to recover it. The 60th term has 180 decimal digits.

The longest integer coefficient appearing in the recurrence has only 20 decimal digits.

For example, the numbers on the previous slide satisfy a recurrence of order 4 and degree 10.

Around 60 terms are needed to recover it. The 60th term has 180 decimal digits.

The longest integer coefficient appearing in the recurrence has only 20 decimal digits.

The exact recurrence can be recovered from homomorphic images of the first 60 terms.

0
170
57125
48268101
34260690332
28950283288564
24602777889341700
21958748103044947821
19982460773770890734814
18589778412414172744395308
17556405435959384905586216420
16804193264871415986848637912866
16258906633984352510780895055898688
15878645003134966488517342432611820340
15631047178991661938104976711572278528840
15494275516175484896146558165069374931768650
15452119731275448721521690374123048169473745090
15492944429910290948927453354128640277129701928270
15608195638318139575397871729737310479957231181434400
15791696434663015062086294548870131152897244600962599710
16039042304161558566190267565720083550110055872936313121300
16347221676787084843566201114528305144441011394615536628043480
16714327636344626391862041955812314792830121148741093212135914440
17139356963672793388669217006249699836555901801582671305065963412450
17622061542861347959625369356680682135593177881983900768539311826713472
18162841216793283422562091421291078521630723657702122424507756283808698700
18762665614999822007839830386311098144372506555360938018652662698220539694616
19423018217659251266276892430699632002229719351100435132025989366139940897600008
20145857126504814155109603745644558012097546254998545662831506345299150654223844360
20933588899340997857198064126985453367261304123281113854543929397365087045753567548888
21789052707980917749010589339181187870108450716708413481060716254608148803460083665644160

mod	18446744073709551557
	0
	170
	57125
	48268101
	34260690332
	28950283288564
	24602777889341700
	3512004029335396264
	4636941943446398583
	16731901151034173887
	13561571021375624155
	18327681355361409199
	14135275161253345008
	5637819232275028612
	6637602357189385604
	12482169677218181673
	13064253343726879423
	14625225362239686504
	10738834608406986658
	961106949064586405
	2211804365157896289
	8829591048746708080
	15009988290858134393
	7627367407386026140
	14734287943773226198
	15483359934879899009
	899837740350271794
	6952192533371026338
	17697300886138518812
	14174304902082598370
	9566720042687775664

not needed

But there is a catch: the guessed recurrence is not unique. Instead, all the correct recurrences form a vector space.

But there is a catch: the guessed recurrence is not unique. Instead, all the correct recurrences form a vector space.

Chinese remaindering will only succeed if we apply it to recurrences sharing the same homomorphic preimage.

But there is a catch: the guessed recurrence is not unique. Instead, all the correct recurrences form a vector space.

Chinese remaindering will only succeed if we apply it to recurrences sharing the same homomorphic preimage.

We could ensure a unique preimage by normalizing a specific coefficient of the recurrence to 1.

But there is a catch: the guessed recurrence is not unique. Instead, all the correct recurrences form a vector space.

Chinese remaindering will only succeed if we apply it to recurrences sharing the same homomorphic preimage.

We could ensure a unique preimage by normalizing a specific coefficient of the recurrence to 1.

But then we must be prepared that the coefficients of the preimage live in $\mathbb{Q}$ rather than $\mathbb{Z}$.

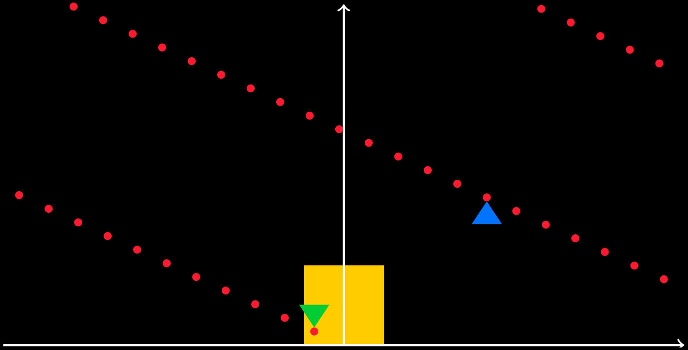
Rational reconstruction comes to rescue: given $m \in \mathbb{Z}$ and $x \in \mathbb{Z}$, we can find small $p, q \in \mathbb{Z}$ such that $\frac{p}{q} \equiv x \bmod m$.

Rational reconstruction comes to rescue: given $m \in \mathbb{Z}$ and $x \in \mathbb{Z}$, we can find small $p, q \in \mathbb{Z}$ such that $\frac{p}{q} \equiv x \bmod m$.

Of course, such p, q are not uniquely determined, but we can be sure to find the right answer when $m > \max(4p^2, q^2)$.

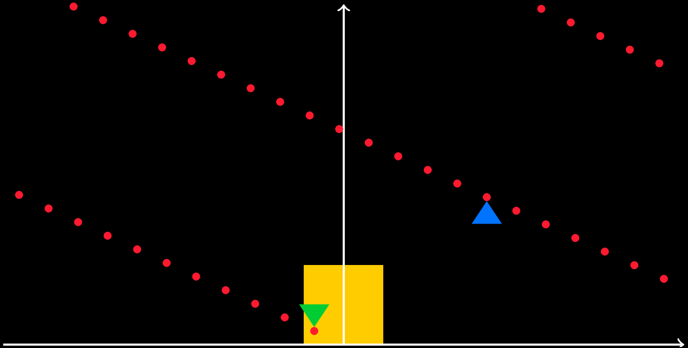
Rational reconstruction comes to rescue: given $m \in \mathbb{Z}$ and $x \in \mathbb{Z}$, we can find small $p, q \in \mathbb{Z}$ such that $\frac{p}{q} \equiv x \bmod m$.

Of course, such p, q are not uniquely determined, but we can be sure to find the right answer when $m > \max(4p^2, q^2)$.



Rational reconstruction comes to rescue: given $m \in \mathbb{Z}$ and $x \in \mathbb{Z}$, we can find small $p, q \in \mathbb{Z}$ such that $\frac{p}{q} \equiv x \bmod m$.

Of course, such p, q are not uniquely determined, but we can be sure to find the right answer when $m > \max(4p^2, q^2)$.

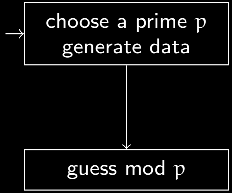


Here is how you should do guessing for large examples.

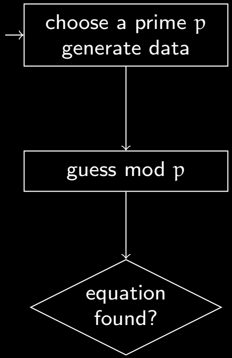
Here is how you should do guessing for large examples.

$\rightarrow$ $\boxed{\text{choose a prime } p \\ \text{generate data}}$

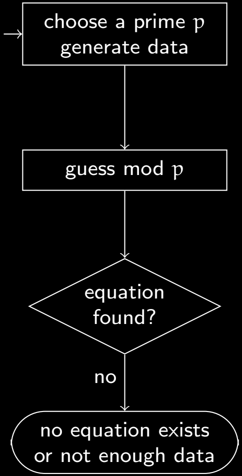
Here is how you should do guessing for large examples.



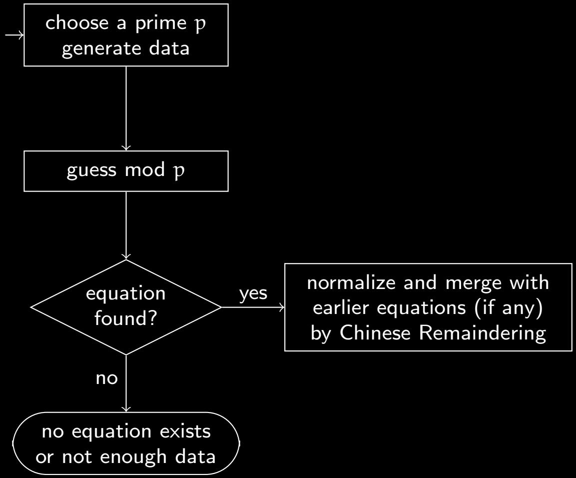
Here is how you should do guessing for large examples.



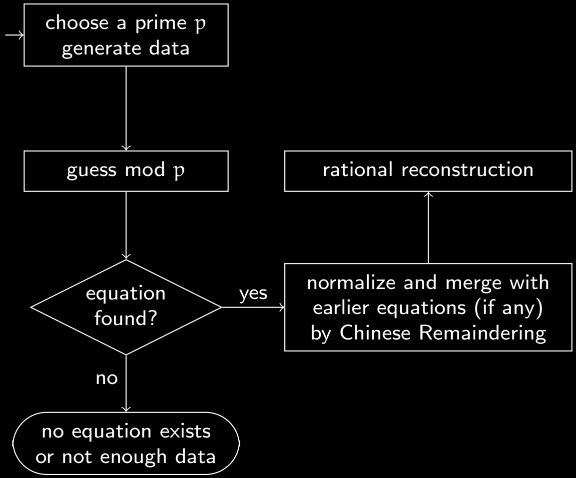
Here is how you should do guessing for large examples.



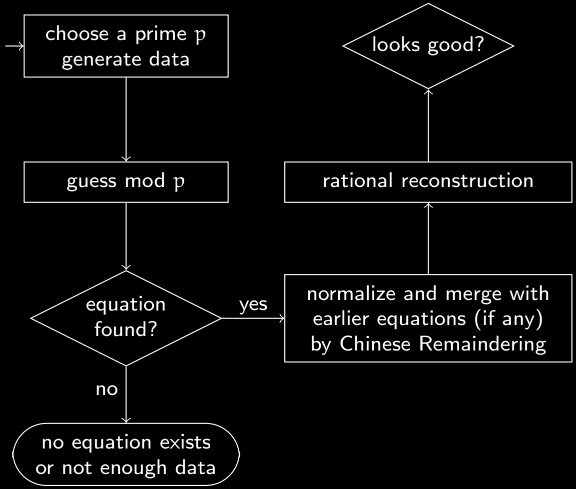
Here is how you should do guessing for large examples.



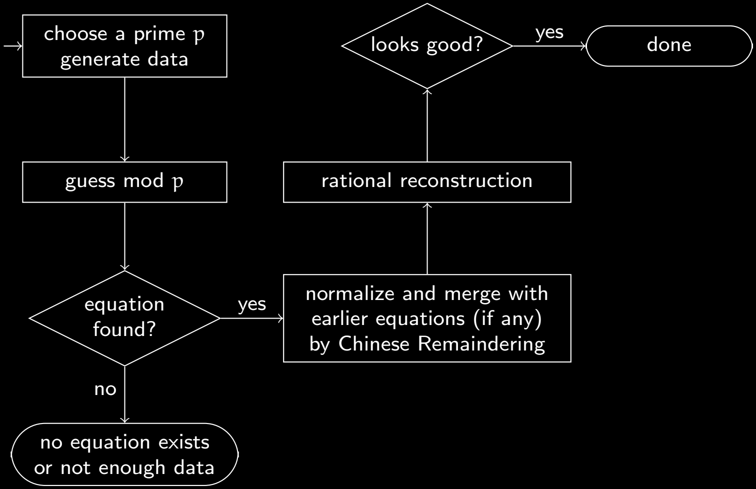
Here is how you should do guessing for large examples.



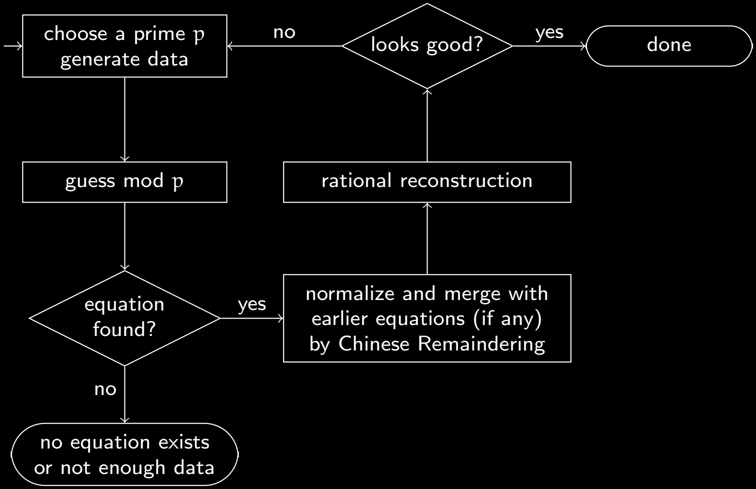
Here is how you should do guessing for large examples.



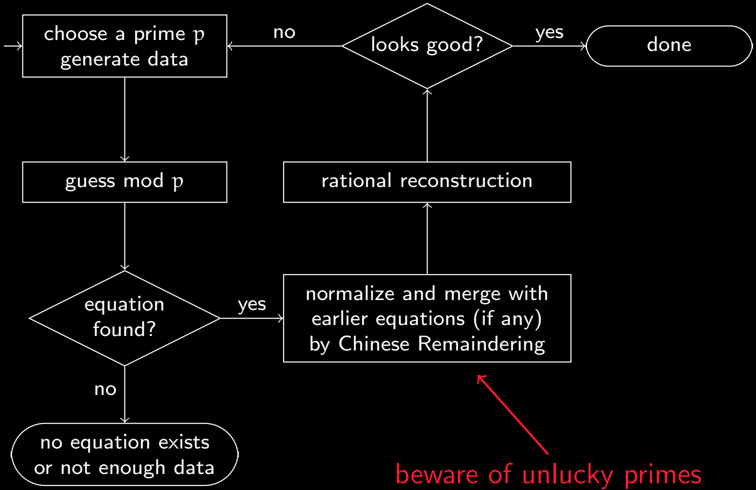
Here is how you should do guessing for large examples.



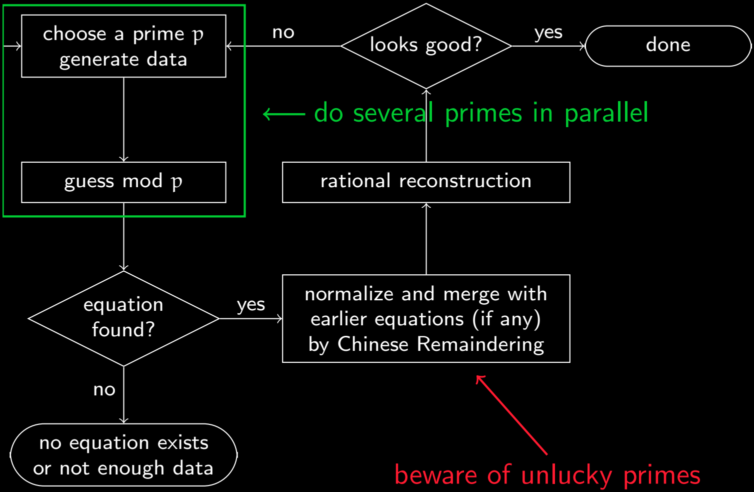
Here is how you should do guessing for large examples.



Here is how you should do guessing for large examples.



Here is how you should do guessing for large examples.



When there are also parameters, also use evaluation/interpolation and rational function reconstruction.

$$
\begin{tikzcd}
\mathbb{Q}(x) \arrow[rrrrr, "\text{solve}"] \arrow[d, "\text{mod}"'] & & & & & \mathbb{Q}(x) \\
\mathbb{Z}_p(x) \arrow[dr, "\text{eval}"'] & & & & & \mathbb{Z}(x) \arrow[u, "\text{rr}"'] \\
& \mathbb{Z}_p \arrow[dr, "\text{solve}"'] & & & \mathbb{Z}_p(x) \arrow[ur, "\text{cra}"'] & \\
& & \mathbb{Z}_p \arrow[r, "\text{interpol}"'] & \mathbb{Z}_p[x] \arrow[ur, "\text{rr}"'] & &
\end{tikzcd}
$$

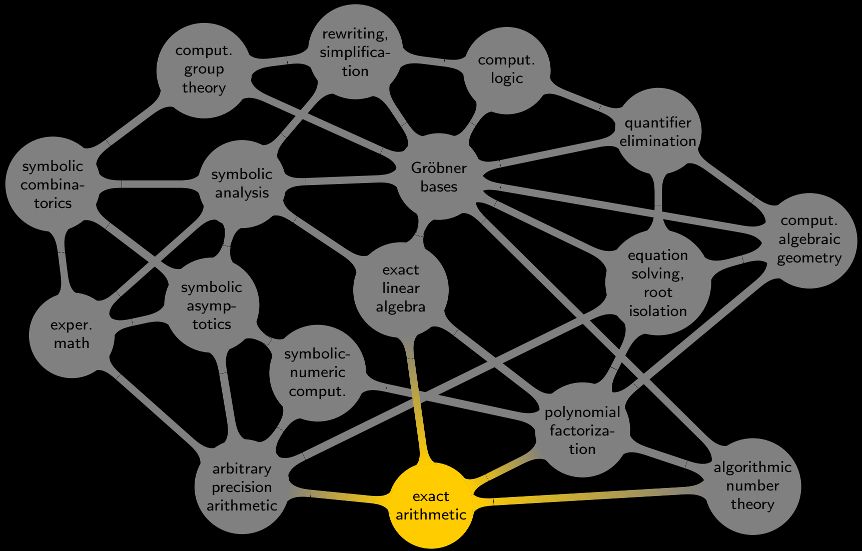
Lesson 3: Sometimes it's faster to take a detour

Exercises.

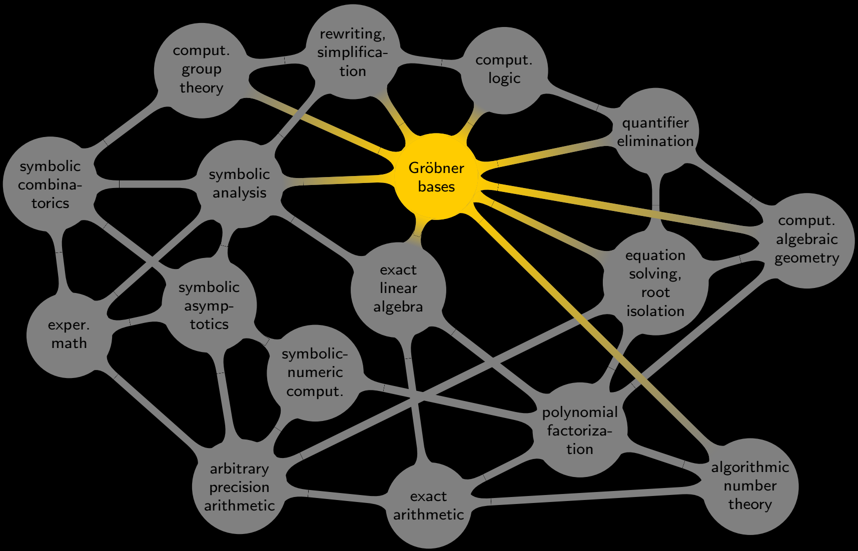
- If $F(n)$ is the nth Fibonacci number, then $F(2^{1000})$ is an integer with 10^{300} decimal digits. Determine the 20 least significant decimal digits of $F(2^{1000})$.

- Fix a random matrix $A \in \mathbb{Z}^{100\times 101}$ and a set of primes $p_1, \ldots, p_{100}$ with $p_i \approx 2^i$. For each i check how long your computer needs to find a basis of $\ker A$ mod p_i.

- Use Chinese remaindering and rational reconstruction to find a basis vector of $\ker A$ in $\mathbb{Q}^{101}$. How can we tell in advance how many primes are needed?



https://tinyurl.com/y8h6l6sp


comput. group theory
rewriting, simplifica- tion
comput. logic
quantifier elimination
symbolic combina- torics
symbolic analysis
Gröbner bases
comput. algebraic geometry
equation solving, root isolation
exact linear algebra
symbolic asymp- totics
exper. math
symbolic- numeric comput.
polynomial factoriza- tion
arbitrary precision arithmetic
exact arithmetic
algorithmic number theory

Finite sets of numbers can be viewed as solutions of polynomial equations:

Finite sets of numbers can be viewed as solutions of polynomial equations:

$p = (x-1)(x-2)(x-4) = 0$

Finite sets of numbers can be viewed as solutions of polynomial equations:

$p = (x-1)(x-2)(x-4) = 0$

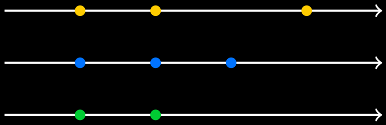
$q = (x-1)(x-2)(x-3) = 0$

Finite sets of numbers can be viewed as solutions of polynomial equations:

$p = (x-1)(x-2)(x-4) = 0$

$q = (x-1)(x-2)(x-3) = 0$

Intersection: $\gcd(p, q) = 0$



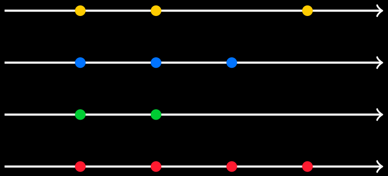
Finite sets of numbers can be viewed as solutions of polynomial equations:

$p = (x-1)(x-2)(x-4) = 0$

$q = (x-1)(x-2)(x-3) = 0$

Intersection: $\gcd(p, q) = 0$

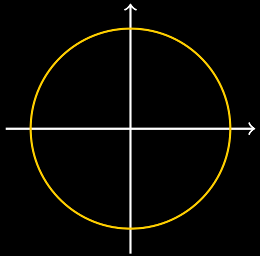
Union: $\operatorname{lcm}(p, q) = 0$



In the case of two variables, the solution set of a single polynomial is a curve.

In the case of two variables, the solution set of a single polynomial is a curve.

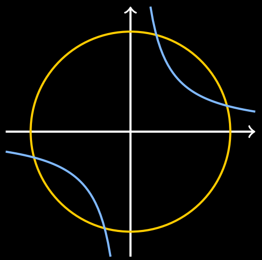
$$x^2 + y^2 - 4 = 0$$



In the case of two variables, the solution set of a single polynomial is a curve.

$$x^2 + y^2 - 4 = 0$$

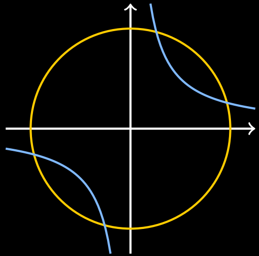
$$xy - 1 = 0$$



In the case of two variables, the solution set of a single polynomial is a curve.

$$x^2 + y^2 - 4 = 0$$

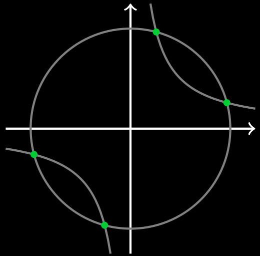
$$xy - 1 = 0$$



Any finite set of points can be viewed as the intersection of such curves.

In the case of two variables, the solution set of a single polynomial is a curve.

$$\begin{gathered} x^2 + y^2 - 4 = 0 \\ \wedge \\ xy - 1 = 0 \end{gathered}$$



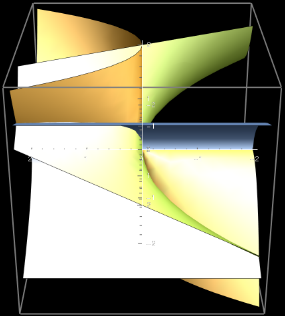
Any finite set of points can be viewed as the intersection of such curves.

A polynomial in three variables describes a surface.

$$xz - y^2 = 0$$

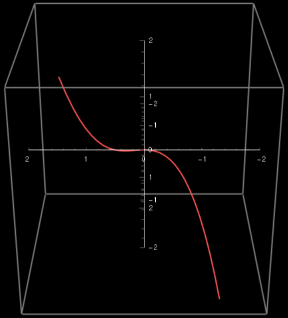
$$y - z^2 = 0$$

$$x - yz = 0$$



A polynomial in three variables describes a surface.

$$
\begin{gathered}
xz - y^2 = 0 \\
\wedge \\
y - z^2 = 0 \\
\wedge \\
x - yz = 0
\end{gathered}
$$



Curves and finite sets of points can be viewed as intersections of such surfaces.

Typical questions about systems of polynomial equations:

Typical questions about systems of polynomial equations:

- Decide whether a system of equations is inconsistent

Typical questions about systems of polynomial equations:

- Decide whether a system of equations is inconsistent
- When it's inconsistent, construct a proof certificate

Typical questions about systems of polynomial equations:

- Decide whether a system of equations is inconsistent
- When it's inconsistent, construct a proof certificate
- When it's consistent, determine the number of solutions

Typical questions about systems of polynomial equations:

- Decide whether a system of equations is inconsistent
- When it's inconsistent, construct a proof certificate
- When it's consistent, determine the number of solutions
- When there are finitely many solutions, list them

Typical questions about systems of polynomial equations:

- Decide whether a system of equations is inconsistent
- When it's inconsistent, construct a proof certificate
- When it's consistent, determine the number of solutions
- When there are finitely many solutions, list them
- When the solution set is infinite, determine its dimension

Typical questions about systems of polynomial equations:

- Decide whether a system of equations is inconsistent
- When it's inconsistent, construct a proof certificate
- When it's consistent, determine the number of solutions
- When there are finitely many solutions, list them
- When the solution set is infinite, determine its dimension
- Decide whether one system of equations implies another

Typical questions about systems of polynomial equations:

- Decide whether a system of equations is inconsistent
- When it's inconsistent, construct a proof certificate
- When it's consistent, determine the number of solutions
- When there are finitely many solutions, list them
- When the solution set is infinite, determine its dimension
- Decide whether one system of equations implies another
- Decide whether two polynomial functions agree on a variety

Typical questions about systems of polynomial equations:

- Decide whether a system of equations is inconsistent
- When it's inconsistent, construct a proof certificate
- When it's consistent, determine the number of solutions
- When there are finitely many solutions, list them
- When the solution set is infinite, determine its dimension
- Decide whether one system of equations implies another
- Decide whether two polynomial functions agree on a variety
- Eliminate some variables from a given equation system

Typical questions about systems of polynomial equations:

- Decide whether a system of equations is inconsistent
- When it's inconsistent, construct a proof certificate
- When it's consistent, determine the number of solutions
- When there are finitely many solutions, list them
- When the solution set is infinite, determine its dimension
- Decide whether one system of equations implies another
- Decide whether two polynomial functions agree on a variety
- Eliminate some variables from a given equation system
- Compute kernels and images of polynomial homomorphisms

Typical questions about systems of polynomial equations:

- Decide whether a system of equations is inconsistent
- When it's inconsistent, construct a proof certificate
- When it's consistent, determine the number of solutions
- When there are finitely many solutions, list them
- When the solution set is infinite, determine its dimension
- Decide whether one system of equations implies another
- Decide whether two polynomial functions agree on a variety
- Eliminate some variables from a given equation system
- Compute kernels and images of polynomial homomorphisms

All these questions can be answered using Gröbner bases.

Lesson 4: Gröbner bases can not only solve nonlinear systems

Polynomial equations have implications:

$$p = 0 \text{ and } q = 0 \Rightarrow p + q = 0$$
$$p = 0 \text{ and } q \text{ arbitrary} \Rightarrow pq = 0.$$

Polynomial equations have implications:

$$p = 0 \text{ and } q = 0 \Rightarrow p + q = 0$$
$$p = 0 \text{ and } q \text{ arbitrary} \Rightarrow pq = 0.$$

Given $p_1, \ldots, p_k \in K[x_1, \ldots, x_n]$, we therefore consider

$$\langle p_1, \ldots, p_k \rangle := \big\{ q_1 p_1 + \cdots + q_k p_k : q_1, \ldots, q_k \in K[x_1, \ldots, x_n] \big\},$$

the ideal generated by $p_1, \ldots, p_k$ in the ring $K[x_1, \ldots, x_n]$. We call $\{p_1, \ldots, p_k\}$ a basis of the ideal.

Polynomial equations have implications:

$$p = 0 \text{ and } q = 0 \Rightarrow p + q = 0$$
$$p = 0 \text{ and } q \text{ arbitrary} \Rightarrow pq = 0.$$

Given $p_1, \ldots, p_k \in K[x_1, \ldots, x_n]$, we therefore consider

$$\langle p_1, \ldots, p_k \rangle := \{ q_1 p_1 + \cdots + q_k p_k : q_1, \ldots, q_k \in K[x_1, \ldots, x_n] \},$$

the ideal generated by $p_1, \ldots, p_k$ in the ring $K[x_1, \ldots, x_n]$. We call $\{p_1, \ldots, p_k\}$ a basis of the ideal.

Intuition: the ideal is a "theory" of equations of the form "poly $= 0$" in which $p_1, \ldots, p_k$ are the "axioms" and implications quoted above are the "deduction rules".

The basis of an ideal is not unique.

The basis of an ideal is not unique.

Example: $\langle x^2 + y^2 - 4,\ \ xy - 1\rangle = \langle y^4 - 4y^2 + 1,\ \ y^3 - 4y + x\rangle$.

The basis of an ideal is not unique.

Example: $\langle x^2 + y^2 - 4,\ \ xy - 1\rangle = \langle y^4 - 4y^2 + 1,\ \ y^3 - 4y + x\rangle.$

Proof:

The basis of an ideal is not unique.

Example: $\langle \underbrace{x^2 + y^2 - 4}_{p_1},\ \underbrace{xy - 1}_{p_2} \rangle = \langle \underbrace{y^4 - 4y^2 + 1}_{q_1},\ \underbrace{y^3 - 4y + x}_{q_2} \rangle.$

Proof:

The basis of an ideal is not unique.

Example: $\langle \underbrace{x^2+y^2-4}_{p_1},\ \underbrace{xy-1}_{p_2} \rangle = \langle \underbrace{y^4-4y^2+1}_{q_1},\ \underbrace{y^3-4y+x}_{q_2} \rangle.$

Proof:

"$\subseteq$" $\quad p_1 = (y^2-4)\,q_1 + (x+4y-y^3)\,q_2,$

$\quad\quad p_2 = -q_1 + y\,q_2.$

The basis of an ideal is not unique.

Example: $\langle \underbrace{x^2+y^2-4}_{p_1},\ \underbrace{xy-1}_{p_2} \rangle = \langle \underbrace{y^4-4y^2+1}_{q_1},\ \underbrace{y^3-4y+x}_{q_2} \rangle$.

Proof:

"$\subseteq$" $\quad p_1 = (y^2-4)\, q_1 + (x+4y-y^3)\, q_2,$
$\quad p_2 = -q_1 + y\, q_2.$

"$\supseteq$" $\quad q_1 = y^2\, p_1 - (xy+1)\, p_2,$
$\quad q_2 = y\, p_1 - x\, p_2.$ ∎

The basis of an ideal is not unique.

Example: $\langle \underbrace{x^2 + y^2 - 4}_{p_1},\ \underbrace{xy - 1}_{p_2} \rangle = \langle \underbrace{y^4 - 4y^2 + 1}_{q_1},\ \underbrace{y^3 - 4y + x}_{q_2} \rangle$.

Proof:

"$\subseteq$" $\quad p_1 = (y^2 - 4)\, q_1 + (x + 4y - y^3)\, q_2,$

$\quad\quad p_2 = -q_1 + y\, q_2.$

"$\supseteq$" $\quad q_1 = y^2\, p_1 - (xy + 1)\, p_2,$

$\quad\quad q_2 = y\, p_1 - x\, p_2. \quad \blacksquare$

Among all the bases of a given ideal, the Gröbner basis is one that satisfies a certain minimality condition.

For $n > 1$, divisibility on the set of monomials $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ is no longer a total ordering, e.g., x^2y and xy^2 are not comparable.

For $n > 1$, divisibility on the set of monomials $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ is no longer a total ordering, e.g., x^2y and xy^2 are not comparable.

Fix a total ordering on the monomials which is compatible with divisibility. Such an order is called a term order.

For $n > 1$, divisibility on the set of monomials $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ is no longer a total ordering, e.g., $x^2 y$ and xy^2 are not comparable.

Fix a total ordering on the monomials which is compatible with divisibility. Such an order is called a term order.

Once a term order is chosen, every nonzero polynomial has a unique maximal term, called the head or the leading term.

For $n > 1$, divisibility on the set of monomials $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ is no longer a total ordering, e.g., x^2y and xy^2 are not comparable.

Fix a total ordering on the monomials which is compatible with divisibility. Such an order is called a term order.

Once a term order is chosen, every nonzero polynomial has a unique maximal term, called the head or the leading term.

Example: $\boxed{3x^3y^2} + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17.$

For $n > 1$, divisibility on the set of monomials $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ is no longer a total ordering, e.g., x^2y and xy^2 are not comparable.

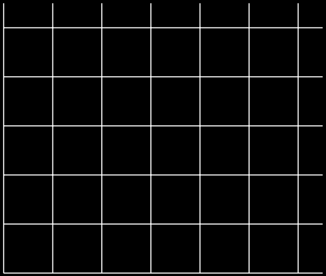
Fix a total ordering on the monomials which is compatible with divisibility. Such an order is called a term order.

Once a term order is chosen, every nonzero polynomial has a unique maximal term, called the head or the leading term.

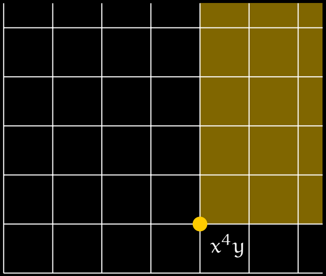
Example: $\boxed{3x^3y^2} + 7x^2y^3 + 8x^2y - 4xy + 8y^3 - 17.$

Among all the bases of an ideal, the Gröbner basis is such that the leading terms of its elements are as small as possible.

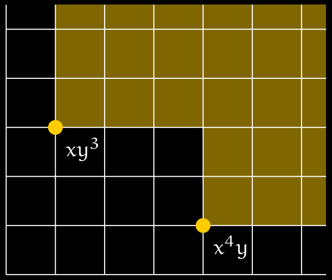
If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.



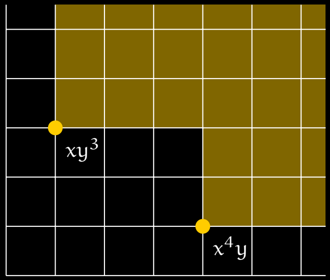
If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.



If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.

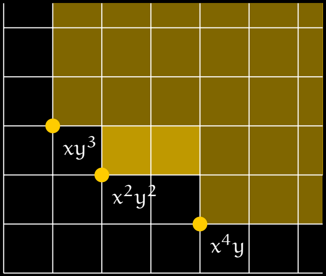


If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.



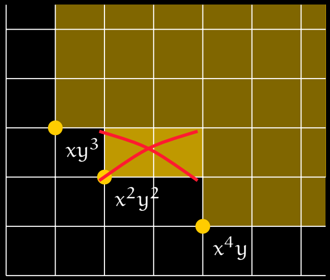
In general however, the ideal may also contain polynomials whose head is not a multiple of the head of any basis element.

If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.



In general however, the ideal may also contain polynomials whose head is not a multiple of the head of any basis element.

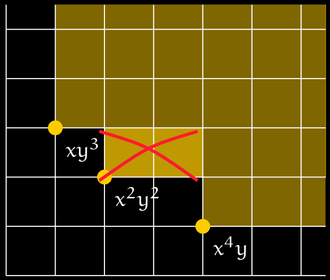
If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.



In general however, the ideal may also contain polynomials whose head is not a multiple of the head of any basis element.

The basis is called a Gröbner basis if this does not happen.

If a basis of an ideal has a polynomial with head h, then every multiple of h is the head of some element of I.



In general however, the ideal may also contain polynomials whose head is not a multiple of the head of any basis element.

$\{g_1, \ldots, g_k\}$ is a Gröbner basis $\iff$
$\forall\ p \in \langle g_1, \ldots, g_k\rangle \setminus \{0\}\ \exists\ i \in \{1, \ldots, k\} : \mathrm{Head}(g_i) \mid \mathrm{Head}(p)$.

Fix an ideal $I \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ and define

$$p \sim q \iff p - q \in I.$$

Fix an ideal $I \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ and define

$$p \sim q \iff p - q \in I.$$

Then $\mathbb{Q}[x_1, \ldots, x_n]/{\sim} = \mathbb{Q}[x_1, \ldots, x_n]/I$ is a ring.

Fix an ideal $I \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ and define

$$p \sim q \iff p - q \in I.$$

Then $\mathbb{Q}[x_1, \ldots, x_n]/\sim = \mathbb{Q}[x_1, \ldots, x_n]/I$ is a ring.

Its elements can be interpreted as polynomial functions restricted to the zero set of I.

Fix an ideal $I \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ and define

$$p \sim q \iff p - q \in I.$$

Then $\mathbb{Q}[x_1, \ldots, x_n]/\sim\ = \mathbb{Q}[x_1, \ldots, x_n]/I$ is a ring.

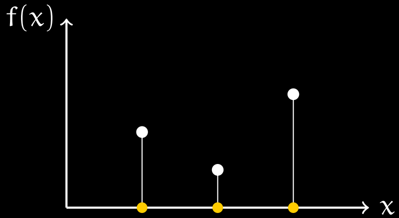
Its elements can be interpreted as polynomial functions restricted to the zero set of I.

Fix an ideal $I \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ and define

$$p \sim q \iff p - q \in I.$$

Then $\mathbb{Q}[x_1, \ldots, x_n]/\sim = \mathbb{Q}[x_1, \ldots, x_n]/I$ is a ring.

Its elements can be interpreted as polynomial functions restricted to the zero set of I.

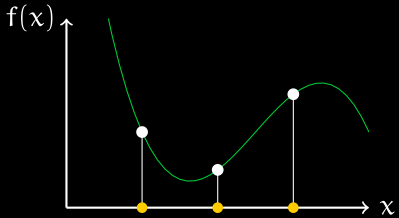


Fix an ideal $I \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ and define

$$p \sim q \iff p - q \in I.$$

Then $\mathbb{Q}[x_1, \ldots, x_n]/\sim \, = \mathbb{Q}[x_1, \ldots, x_n]/I$ is a ring.

Its elements can be interpreted as polynomial functions restricted to the zero set of I.

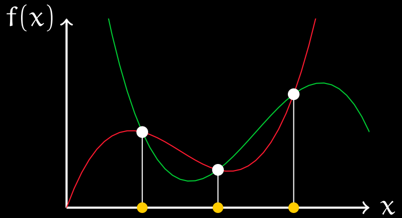


Fix an ideal $I \subseteq \mathbb{Q}[x_1, \dots, x_n]$ and define

$$p \sim q \iff p - q \in I.$$

Then $\mathbb{Q}[x_1, \dots, x_n]/{\sim} = \mathbb{Q}[x_1, \dots, x_n]/I$ is a ring.

Its elements can be interpreted as polynomial functions restricted to the zero set of I.

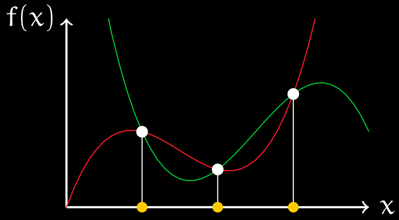


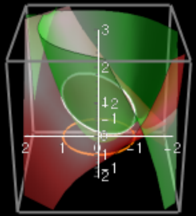
Fix an ideal $I \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ and define

$$p \sim q \iff p - q \in I.$$

Then $\mathbb{Q}[x_1, \ldots, x_n]/\sim \; = \mathbb{Q}[x_1, \ldots, x_n]/I$ is a ring.

Its elements can be interpreted as polynomial functions restricted to the zero set of I.





Fix an ideal $I \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ and define

$$p \sim q \iff p - q \in I.$$

Then $\mathbb{Q}[x_1, \ldots, x_n]/\sim \, = \mathbb{Q}[x_1, \ldots, x_n]/I$ is a ring.

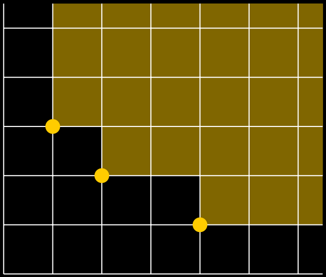
As a $\mathbb{Q}$-vector space, it is generated by the classes of all terms that are not divided by the head of a basis element.

Fix an ideal $I \subseteq \mathbb{Q}[x_1, \dots, x_n]$ and define

$$p \sim q \iff p - q \in I.$$

Then $\mathbb{Q}[x_1, \dots, x_n]/\!\sim\, = \mathbb{Q}[x_1, \dots, x_n]/I$ is a ring.

As a $\mathbb{Q}$-vector space, it is generated by the classes of all terms that are not divided by the head of a basis element.

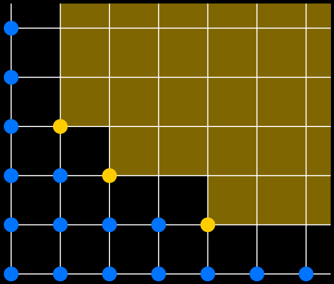


Fix an ideal $I \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ and define

$$p \sim q \iff p - q \in I.$$

Then $\mathbb{Q}[x_1, \ldots, x_n]/\sim = \mathbb{Q}[x_1, \ldots, x_n]/I$ is a ring.

As a $\mathbb{Q}$-vector space, it is generated by the classes of all terms that are not divided by the head of a basis element.

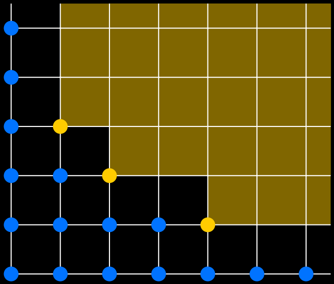


Fix an ideal $I \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ and define

$$p \sim q \iff p - q \in I.$$

Then $\mathbb{Q}[x_1, \ldots, x_n]/{\sim} = \mathbb{Q}[x_1, \ldots, x_n]/I$ is a ring.

The ideal basis is a Gröbner basis iff the blue terms form a vector space basis of $\mathbb{Q}[x_1, \ldots, x_n]/I$.



- Every equivalence class contains at least one polynomial with only blue terms.

- Every equivalence class contains at least one polynomial with only blue terms.
- We have a Gröbner basis if and only if every equivalence class contains exactly one such polynomial.

- Every equivalence class contains at least one polynomial with only blue terms.
- We have a Gröbner basis if and only if every equivalence class contains exactly one such polynomial.
- This polynomial is then called the normal form of any polynomial in the class.

- Every equivalence class contains at least one polynomial with only blue terms.
- We have a Gröbner basis if and only if every equivalence class contains exactly one such polynomial.
- This polynomial is then called the normal form of any polynomial in the class.
- There is an algorithm for computing the normal form of p w.r.t. a given Gröbner basis G.

- Every equivalence class contains at least one polynomial with only blue terms.
- We have a Gröbner basis if and only if every equivalence class contains exactly one such polynomial.
- This polynomial is then called the normal form of any polynomial in the class.
- There is an algorithm for computing the normal form of p w.r.t. a given Gröbner basis G.
- We have $p \in \langle G \rangle$ if and only if the normal form of p w.r.t. G is zero.

- Given any basis of an ideal I, we can compute a Gröbner basis of the ideal.

- Given any basis of an ideal I, we can compute a Gröbner basis of the ideal.
- In terms of complexity theory, the computation of a Gröbner basis is a hard problem.

- Given any basis of an ideal I, we can compute a Gröbner basis of the ideal.
- In terms of complexity theory, the computation of a Gröbner basis is a hard problem.
- In practice, the situation is often not as bad as one could expect, mainly for two reasons:

- Given any basis of an ideal I, we can compute a Gröbner basis of the ideal.
- In terms of complexity theory, the computation of a Gröbner basis is a hard problem.
- In practice, the situation is often not as bad as one could expect, mainly for two reasons:
- 1. Many problems arising in practice do not exhibit worst case behaviour.

- Given any basis of an ideal I, we can compute a Gröbner basis of the ideal.
- In terms of complexity theory, the computation of a Gröbner basis is a hard problem.
- In practice, the situation is often not as bad as one could expect, mainly for two reasons:
- 1. Many problems arising in practice do not exhibit worst case behaviour.
- 2. Much effort has been invested into efficient algorithms and software.

Lesson 5: Computing a Gröbner basis is not hopeless

With a Gröbner basis at hand, everything about the ideal is known.

With a Gröbner basis at hand, everything about the ideal is known.

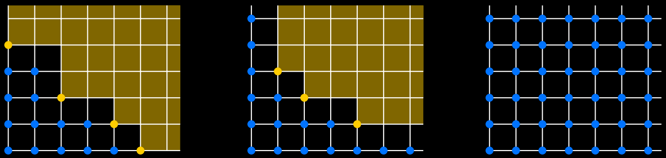
For example, you can get the dimension of its zero set by counting how many blue terms* there are up to degree N, as $N \to \infty$.

---

* only works for suitably chosen term orders.

With a Gröbner basis at hand, everything about the ideal is known.

For example, you can get the dimension of its zero set by counting how many blue terms* there are up to degree N, as $N \to \infty$.

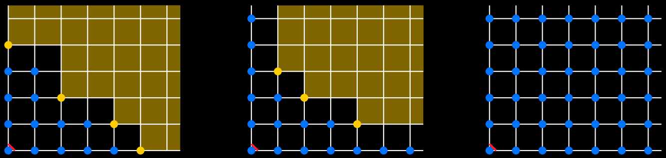


---

* only works for suitably chosen term orders.

With a Gröbner basis at hand, everything about the ideal is known.

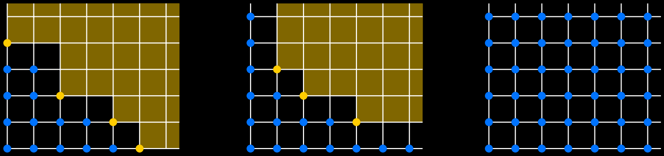
For example, you can get the dimension of its zero set by counting how many blue terms* there are up to degree N, as $N \to \infty$.



* only works for suitably chosen term orders.

With a Gröbner basis at hand, everything about the ideal is known.

For example, you can get the dimension of its zero set by counting how many blue terms* there are up to degree N, as $N \to \infty$.



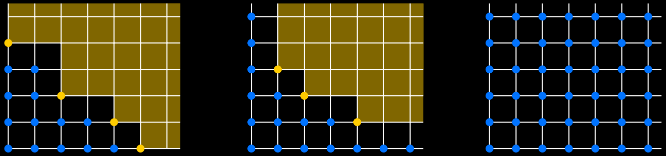
$\dim(I) = 0$ $\quad$ $\dim(I) = 1$ $\quad$ $\dim(I) = 2$

---

* only works for suitably chosen term orders.

With a Gröbner basis at hand, everything about the ideal is known.

For example, you can get the dimension of its zero set by counting how many blue terms* there are up to degree N, as $N \to \infty$.



$\dim(I) = 0$ isolated points

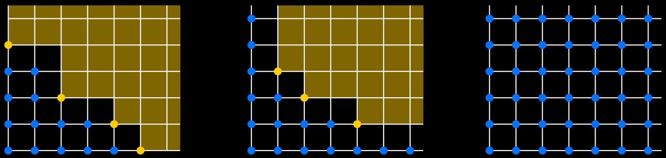
$\dim(I) = 1$ curves

$\dim(I) = 2$ surfaces

* only works for suitably chosen term orders.

With a Gröbner basis at hand, everything about the ideal is known.

For example, you can get the dimension of its zero set by counting how many blue terms* there are up to degree N, as $N \to \infty$.



$\dim(I) = 0$
isolated points

$\dim(I) = 1$
curves

$\dim(I) = 2$
surfaces

Note: $\dim(I) = 0 \iff \dim \mathbb{Q}[x_1, \ldots, x_n]/I < \infty$.

* only works for suitably chosen term orders.

Very useful: you can also find elements of an ideal which only contain some of the variables.

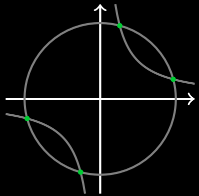
Very useful: you can also find elements of an ideal which only contain some of the variables.

Note: If I is an ideal in $\mathbb{Q}[x, y, z]$, then $I \cap \mathbb{Q}[x, y]$ is an ideal in the smaller ring $\mathbb{Q}[x, y]$.

Very useful: you can also find elements of an ideal which only contain some of the variables.

Note: If I is an ideal in $\mathbb{Q}[x, y, z]$, then $I \cap \mathbb{Q}[x, y]$ is an ideal in the smaller ring $\mathbb{Q}[x, y]$.

Example:



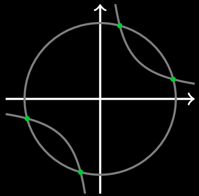
$$\langle x^2 + y^2 - 4, xy - 1 \rangle \cap \mathbb{Q}[x]$$

Very useful: you can also find elements of an ideal which only contain some of the variables.

Note: If I is an ideal in $\mathbb{Q}[x, y, z]$, then $I \cap \mathbb{Q}[x, y]$ is an ideal in the smaller ring $\mathbb{Q}[x, y]$.

Example:

$$\begin{aligned} &\langle x^2 + y^2 - 4, xy - 1\rangle \cap \mathbb{Q}[x] \\ &= \langle x^4 - 4x^2 + 1\rangle \subseteq \mathbb{Q}[x] \end{aligned}$$

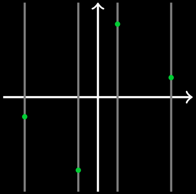


Very useful: you can also find elements of an ideal which only contain some of the variables.

Note: If I is an ideal in $\mathbb{Q}[x, y, z]$, then $I \cap \mathbb{Q}[x, y]$ is an ideal in the smaller ring $\mathbb{Q}[x, y]$.

Example:

$$\begin{aligned} &\langle x^2 + y^2 - 4, xy - 1 \rangle \cap \mathbb{Q}[x] \\ &= \langle x^4 - 4x^2 + 1 \rangle \subseteq \mathbb{Q}[x] \end{aligned}$$

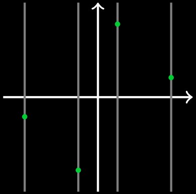


Very useful: you can also find elements of an ideal which only contain some of the variables.

Note: If I is an ideal in $\mathbb{Q}[x, y, z]$, then $I \cap \mathbb{Q}[x, y]$ is an ideal in the smaller ring $\mathbb{Q}[x, y]$.

Example:

$$\begin{aligned}&\langle x^2 + y^2 - 4, xy - 1\rangle \cap \mathbb{Q}[x] \\ &= \langle x^4 - 4x^2 + 1\rangle \subseteq \mathbb{Q}[x]\end{aligned}$$



Fact*: If G is a Gröbner basis of I, then $G \cap \mathbb{Q}[x, y]$ is a Gröbner basis of $I \cap \mathbb{Q}[x, y]$.

* only works for suitably chosen term orders.

Closure properties for algebraic functions via elimination.

Closure properties for algebraic functions via elimination.

Example: Let $f(x), g(x)$ be power series satisfying

$$f(x)^2 - (2x+3)f(x) + 1 = 0, \qquad g(x)^2 + g(x) - x^3 = 0.$$

We want to find a polynomial equation for $h(x) = f(x) + g(x)$.

Closure properties for algebraic functions via elimination.

Example: Let $f(x), g(x)$ be power series satisfying

$$f(x)^2 - (2x+3)f(x) + 1 = 0, \qquad g(x)^2 + g(x) - x^3 = 0.$$

We want to find a polynomial equation for $h(x) = f(x) + g(x)$.

$$\langle f^2 - (2x+3)f + 1,\ g^2 + g - x^3,\ h - (f+g)\rangle \subseteq \mathbb{Q}[x, f, g, h]$$

Closure properties for algebraic functions via elimination.

Example: Let $f(x), g(x)$ be power series satisfying

$$f(x)^2 - (2x+3)f(x) + 1 = 0, \qquad g(x)^2 + g(x) - x^3 = 0.$$

We want to find a polynomial equation for $h(x) = f(x) + g(x)$.

$$\langle f^2 - (2x+3)f + 1,\ g^2 + g - x^3,\ h - (f+g)\rangle \cap \mathbb{Q}[x, h]$$

Closure properties for algebraic functions via elimination.

Example: Let $f(x), g(x)$ be power series satisfying

$$f(x)^2 - (2x+3)f(x) + 1 = 0, \qquad g(x)^2 + g(x) - x^3 = 0.$$

We want to find a polynomial equation for $h(x) = f(x) + g(x)$.

$$\begin{aligned} &\langle f^2 - (2x+3)f + 1,\ g^2 + g - x^3,\ h - (f+g)\rangle \cap \mathbb{Q}[x,h] \\ &= \langle h^4 - 4(x+1)h^3 - (2x^3-4x^2-6x-3)h^2 \\ &\qquad + 2(2x^3+2x+1)(x+1)h + (x+1)^2(x^4-6x^3+x^2-1)\rangle. \end{aligned}$$

Quantifier elimination via elimination.

Quantifier elimination via elimination.

Example: Let $p = x^2 + 2xy + 3y^2$. What conditions must a, b, c satisfy such that there exist α, β with

$$p(\alpha x, \beta y) = ax^2 + bxy + cy^2 \quad ?$$

Quantifier elimination via elimination.

Example: Let $p = x^2 + 2xy + 3y^2$. What conditions must a, b, c satisfy such that there exist α, β with

$$p(\alpha x, \beta y) = ax^2 + bxy + cy^2 \quad ?$$

Coefficient comparison yields:

$$\langle \alpha^2 - a,\ 2\alpha\beta - b,\ 3\beta^2 - c \rangle \subseteq \mathbb{Q}[\alpha, \beta, a, b, c]$$

Quantifier elimination via elimination.

Example: Let $p = x^2 + 2xy + 3y^2$. What conditions must a, b, c satisfy such that there exist α, β with

$$p(\alpha x, \beta y) = ax^2 + bxy + cy^2 \quad ?$$

Coefficient comparison yields:

$$\langle \alpha^2 - a,\ 2\alpha\beta - b,\ 3\beta^2 - c \rangle \cap \mathbb{Q}[a, b, c]$$

Quantifier elimination via elimination.

Example: Let $p = x^2 + 2xy + 3y^2$. What conditions must a, b, c satisfy such that there exist α, β with

$$p(\alpha x, \beta y) = ax^2 + bxy + cy^2 \quad ?$$

Coefficient comparison yields:

$$\langle \alpha^2 - a,\ 2\alpha\beta - b,\ 3\beta^2 - c \rangle \cap \mathbb{Q}[a, b, c]$$
$$= \langle 3b^2 - 4ac \rangle$$

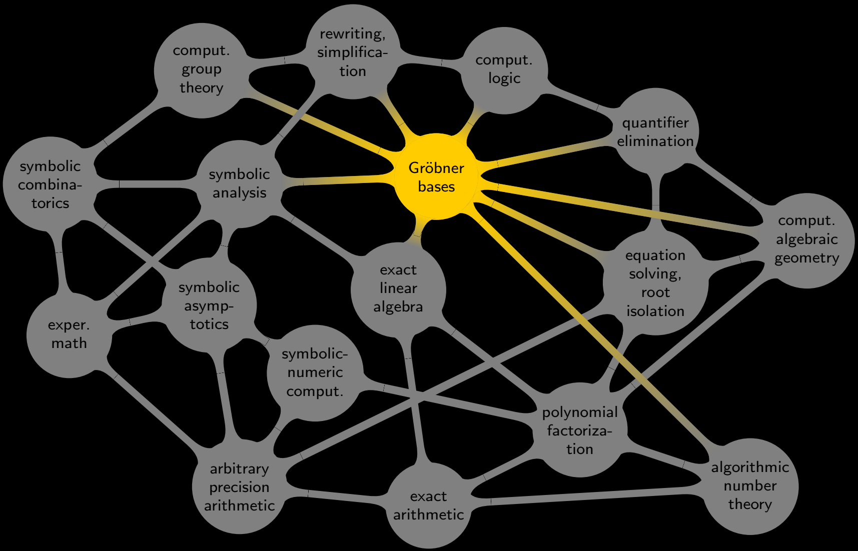
Lesson 6: Gröbner bases are useful

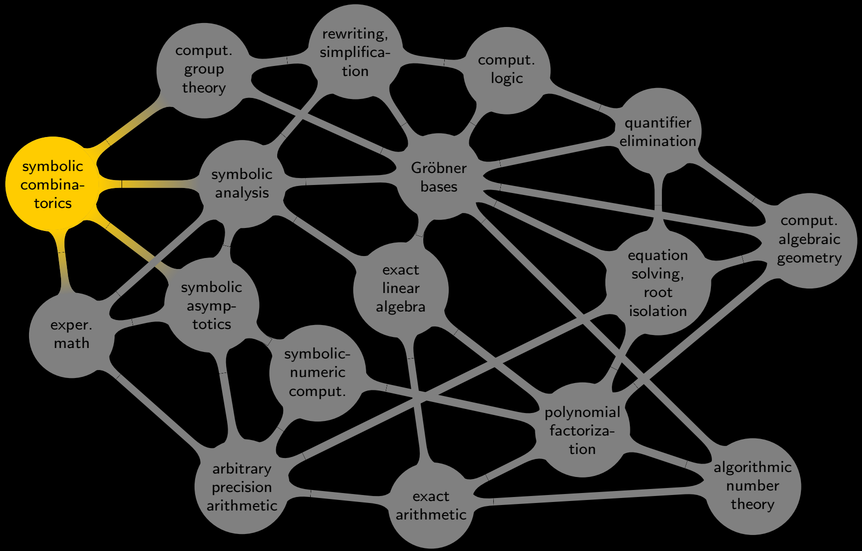
Exercises.

- How long does it take on your computer to compute a Gröbner basis for 3 random polynomials in 4 variables of total degree 5?

- Let $I, J \subseteq \mathbb{Q}[x, y, z]$ be ideals. Show that $I \cap J$ is also an ideal, and that $\dim I = \dim J = 0 \iff \dim(I \cap J) = 0$. What does this mean geometrically?

- Given the minimal polynomials of two algebraic functions $f(x), g(x)$, how can we find the minimal polynomial of their composition $h(x) := f(g(x))$?


comput. group theory
rewriting, simplifica-tion
comput. logic
quantifier elimination
symbolic combina-torics
symbolic analysis
Gröbner bases
comput. algebraic geometry
equation solving, root isolation
exact linear algebra
symbolic asymp-totics
exper. math
symbolic-numeric comput.
polynomial factoriza-tion
arbitrary precision arithmetic
exact arithmetic
algorithmic number theory


comput. group theory
rewriting, simplifica- tion
comput. logic
quantifier elimination
symbolic combina- torics
symbolic analysis
Gröbner bases
comput. algebraic geometry
equation solving, root isolation
exact linear algebra
symbolic asymp- totics
exper. math
symbolic- numeric comput.
polynomial factoriza- tion
arbitrary precision arithmetic
exact arithmetic
algorithmic number theory

Definition.

1 A function $f(x)$ is called D-finite if there exist polynomials $c_0(x), \ldots, c_r(x)$, not all zero, such that

$$c_0(x)f(x) + c_1(x)f'(x) + \cdots + c_r(x)f^{(r)}(x) = 0.$$

2 A sequence $(f_n)_{n=0}^{\infty}$ is called D-finite if there exist polynomials $c_0(n), \ldots, c_r(n)$, not all zero, such that

$$c_0(n)f_n + c_1(n)f_{n+1} + \cdots + c_r(n)f_{n+r} = 0.$$

Definition.

1 A function $f(x)$ is called D-finite if there exist polynomials $c_0(x), \ldots, c_r(x)$, not all zero, such that

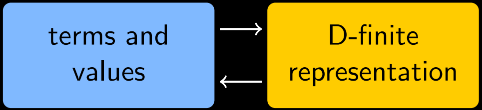
$$c_0(x)f(x) + c_1(x)f'(x) + \cdots + c_r(x)f^{(r)}(x) = 0.$$

2 A sequence $(f_n)_{n=0}^{\infty}$ is called D-finite if there exist polynomials $c_0(n), \ldots, c_r(n)$, not all zero, such that

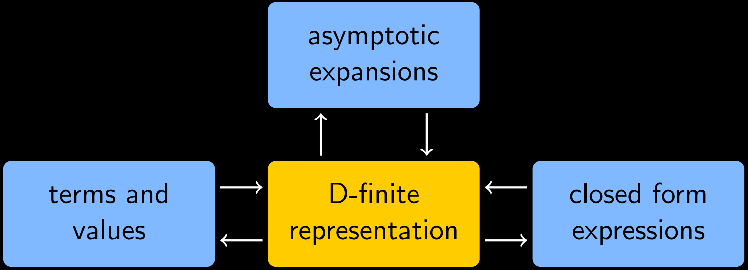
$$c_0(n)f_n + c_1(n)f_{n+1} + \cdots + c_r(n)f_{n+r} = 0.$$

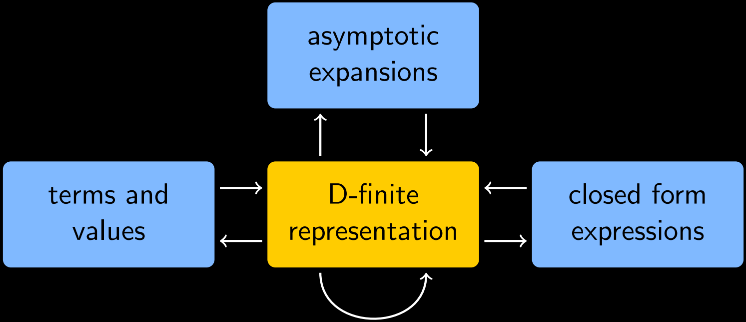
Key feature: a D-finite object is uniquely determined by a defining equation plus a finite number of initial terms.

D-finite representation


terms and values
D-finite representation

$$\begin{tikzcd} \text{terms and values} \arrow[r, shift left] & \text{D-finite representation} \arrow[l, shift left] \arrow[r, shift right] & \text{closed form expressions} \arrow[l, shift right] \end{tikzcd}$$


asymptotic expansions
terms and values
D-finite representation
closed form expressions


asymptotic expansions
terms and values
D-finite representation
closed form expressions

It was already mentioned that D-finite equations can be guessed.

It was already mentioned that D-finite equations can be guessed.

2
5
21
104
565
3255
19488
119712
748341
4735445
30229771
194242152
1254381856
8132826044
52900345680
345022543104
2255449994037
14773402692945
96935423713905
637019314585500
4191982352334315
27619973660237475
182185272080724120
1202945209263916560
7950293909692711200
52588673551755331380
348131918848400963388
2306281394441276650832

It was already mentioned that D-finite equations can be guessed.

2
5
21
104
565
3255
19488
119712
748341
4735445
30229771
194242152
1254381856
8132826044
52900345680
345022543104
2255449994037
14773402692945
96935423713905
637019314585500
4191982352334315
27619973660237475
182185272080724120
1202945209263916560
7950293909692711200
52588673551755331380
348131918848400963388
2306281394441276650832

$$\Rightarrow \quad \begin{aligned}&(1188n^5 + 5346n^4 + 8796n^3 + 6594n^2 + 2268n + 288)f_n\\ &-(473n^5+2365n^4+4453n^3+3899n^2+1554n+216)f_{n+1}\\ &+(44n^5 + 242n^4 + 492n^3 + 454n^2 + 184n + 24)f_{n+2} = 0\end{aligned}$$

It was already mentioned that D-finite equations can be guessed.

2
5
21
104
565
3255
19488
119712
748341
4735445
30229771
194242152
1254381856
8132826044
52900345680
345022543104
2255449994037
14773402692945
96935423713905
637019314585500
4191982352334315
27619973660237475
182185272080724120
1202945209263916560
7950293909692711200
52588673551755331380
348131918848400963388
2306281394441276650832

$$\Rightarrow \quad \begin{aligned} &(1188n^5 + 5346n^4 + 8796n^3 + 6594n^2 + 2268n + 288)f_n \\ &-(473n^5+2365n^4+4453n^3+3899n^2+1554n+216)f_{n+1} \\ &+ (44n^5 + 242n^4 + 492n^3 + 454n^2 + 184n + 24)f_{n+2} = 0 \end{aligned}$$

$$\begin{aligned} &x(4x-1)(27x-4)(6x^2-14x-1)f^{(3)}(x) \\ &+ 6(486x^4 - 1472x^3 + 182x^2 + 24x - 1)f''(x) \\ &+ 12(174x^3 - 636x^2 - 46x + 9)f'(x) \\ &+ 72(x^2 - 6x - 2)f(x) = 0. \end{aligned}$$

Several operations preserve D-finiteness. In particular:

Several operations preserve D-finiteness. In particular:

If f, g are D-finite, then so are $f + g$, and fg.

Several operations preserve D-finiteness. In particular:

If f, g are D-finite, then so are $f + g$, and fg.

If f is a D-finite power series, then

Several operations preserve D-finiteness. In particular:

If f, g are D-finite, then so are $f + g$, and fg.

If f is a D-finite power series, then

- $\int f$ is D-finite

Several operations preserve D-finiteness. In particular:

If f, g are D-finite, then so are $f + g$, and fg.

If f is a D-finite power series, then

- $\int f$ is D-finite
- $f \circ g$ is D-finite for every algebraic(!) function g

Several operations preserve D-finiteness. In particular:

If f, g are D-finite, then so are $f + g$, and fg.

If f is a D-finite power series, then

- $\int f$ is D-finite
- $f \circ g$ is D-finite for every algebraic(!) function g
- if $f(x) = \sum_{n=0}^{\infty} a_n x^n$, then $(a_n)_{n=0}^{\infty}$ is a D-finite sequence.

Several operations preserve D-finiteness. In particular:

If f, g are D-finite, then so are $f + g$, and fg.

If f is a D-finite power series, then

- $\int f$ is D-finite
- $f \circ g$ is D-finite for every algebraic(!) function g
- if $f(x) = \sum_{n=0}^{\infty} a_n x^n$, then $(a_n)_{n=0}^{\infty}$ is a D-finite sequence.

If $(a_n)_{n=0}^{\infty}$ is a D-finite sequence, then

Several operations preserve D-finiteness. In particular:

If f, g are D-finite, then so are $f + g$, and fg.

If f is a D-finite power series, then

- $\int f$ is D-finite
- $f \circ g$ is D-finite for every algebraic(!) function g
- if $f(x) = \sum_{n=0}^{\infty} a_n x^n$, then $(a_n)_{n=0}^{\infty}$ is a D-finite sequence.

If $(a_n)_{n=0}^{\infty}$ is a D-finite sequence, then

- $\left(\sum_{k=0}^{n} a_k\right)_{n=0}^{\infty}$ is D-finite

Several operations preserve D-finiteness. In particular:

If f, g are D-finite, then so are $f + g$, and fg.

If f is a D-finite power series, then

- $\int f$ is D-finite
- $f \circ g$ is D-finite for every algebraic(!) function g
- if $f(x) = \sum_{n=0}^{\infty} a_n x^n$, then $(a_n)_{n=0}^{\infty}$ is a D-finite sequence.

If $(a_n)_{n=0}^{\infty}$ is a D-finite sequence, then

- $\left(\sum_{k=0}^{n} a_k\right)_{n=0}^{\infty}$ is D-finite
- $(a_{un+v})_{n=0}^{\infty}$ is D-finite for every fixed $u, v \in \mathbb{N}$.

Several operations preserve D-finiteness. In particular:

If f, g are D-finite, then so are $f + g$, and fg.

If f is a D-finite power series, then

- $\int f$ is D-finite
- $f \circ g$ is D-finite for every algebraic(!) function g
- if $f(x) = \sum_{n=0}^{\infty} a_n x^n$, then $(a_n)_{n=0}^{\infty}$ is a D-finite sequence.

If $(a_n)_{n=0}^{\infty}$ is a D-finite sequence, then

- $\left(\sum_{k=0}^{n} a_k\right)_{n=0}^{\infty}$ is D-finite
- $(a_{un+v})_{n=0}^{\infty}$ is D-finite for every fixed $u, v \in \mathbb{N}$.
- $f(x) = \sum_{n=0}^{\infty} a_n x^n$ is a D-finite power series

We can use closure properties for turning guesses into theorems.

We can use closure properties for turning guesses into theorems.

Example: The functional equation

$$2xf(x) + e^x(x+1)f(x)^2 + (2x-1)f'(x) = 0$$

has a unique formal power series solution

$$f(x) = 1 + x + 4x^2 + \frac{65}{6}x^3 + \cdots .$$

Is this series D-finite?

We can use closure properties for turning guesses into theorems.

Example: The functional equation

$$2xf(x) + e^x(x+1)f(x)^2 + (2x-1)f'(x) = 0$$

has a unique formal power series solution

$$f(x) = 1 + x + 4x^2 + \tfrac{65}{6}x^3 + \cdots .$$

Is this series D-finite?

Yes, it is. It can be shown using the guess-and-prove paradigm.

- Compute the first ≈ 20 terms of $f(x)$ using the given equation.

- Compute the first ≈ 20 terms of $f(x)$ using the given equation.
- Use them to guess the differential equation

$$\begin{aligned}&(x+1)(2x-1)(x^2+14x-5)f''(x)\\&+(4x^4+65x^3+54x^2+19x-28)f'(x)\\&+2(x^4+18x^3+27x^2+22x-6)f(x)=0.\end{aligned}$$

- Compute the first ≈ 20 terms of $f(x)$ using the given equation.
- Use them to guess the differential equation

$$\begin{aligned}&(x+1)(2x-1)(x^2+14x-5)f''(x)\\&+(4x^4+65x^3+54x^2+19x-28)f'(x)\\&+2(x^4+18x^3+27x^2+22x-6)f(x)=0.\end{aligned}$$

- Let $g(x)$ be the unique power series solution of this differential equation starting like $g(x)=1+x+4x^2+\frac{65}{6}x^3+\cdots$.

- Compute the first ≈ 20 terms of $f(x)$ using the given equation.
- Use them to guess the differential equation

$$\begin{aligned}&(x+1)(2x-1)(x^2+14x-5)f''(x)\\&+(4x^4+65x^3+54x^2+19x-28)f'(x)\\&+2(x^4+18x^3+27x^2+22x-6)f(x)=0.\end{aligned}$$

- Let $g(x)$ be the unique power series solution of this differential equation starting like $g(x)=1+x+4x^2+\frac{65}{6}x^3+\cdots$.
- Use closure properties to prove that

$$2x\ \ g(x)\ \ +\ \ e^x(x+1)\ \ \ g(x)^2\ \ +\ \ (2x-1)\ \ g'(x)\ \ \ =0.$$

- Compute the first ≈ 20 terms of $f(x)$ using the given equation.
- Use them to guess the differential equation

$$\begin{aligned}&(x+1)(2x-1)(x^2+14x-5)f''(x)\\&+(4x^4+65x^3+54x^2+19x-28)f'(x)\\&+2(x^4+18x^3+27x^2+22x-6)f(x)=0.\end{aligned}$$

- Let $g(x)$ be the unique power series solution of this differential equation starting like $g(x)=1+x+4x^2+\frac{65}{6}x^3+\cdots$.
- Use closure properties to prove that

$$2x\ \boxed{g(x)}\ +\ e^x(x+1)\ \boxed{g(x)}^2\ +\ (2x-1)\ g'(x)\ =0.$$

- Compute the first ≈ 20 terms of $f(x)$ using the given equation.
- Use them to guess the differential equation

$$\begin{aligned}&(x+1)(2x-1)(x^2+14x-5)f''(x)\\&+(4x^4+65x^3+54x^2+19x-28)f'(x)\\&+2(x^4+18x^3+27x^2+22x-6)f(x)=0.\end{aligned}$$

- Let $g(x)$ be the unique power series solution of this differential equation starting like $g(x)=1+x+4x^2+\frac{65}{6}x^3+\cdots$.
- Use closure properties to prove that

$$2x\ \boxed{g(x)}\ +\ e^x(x+1)\ \boxed{g(x)}^2\ +\ (2x-1)\ \boxed{g'(x)}\ =0.$$

- Compute the first ≈ 20 terms of $f(x)$ using the given equation.
- Use them to guess the differential equation

$$\begin{aligned}&(x+1)(2x-1)(x^2+14x-5)f''(x)\\&+(4x^4+65x^3+54x^2+19x-28)f'(x)\\&+2(x^4+18x^3+27x^2+22x-6)f(x)=0.\end{aligned}$$

- Let $g(x)$ be the unique power series solution of this differential equation starting like $g(x)=1+x+4x^2+\frac{65}{6}x^3+\cdots$.
- Use closure properties to prove that

$$2x\ \boxed{g(x)}\ +\ e^x(x+1)\ \boxed{\boxed{g(x)}^2}\ +\ (2x-1)\ \boxed{g'(x)}\ =0.$$

- Compute the first ≈ 20 terms of $f(x)$ using the given equation.
- Use them to guess the differential equation

$$\begin{aligned}&(x+1)(2x-1)(x^2+14x-5)f''(x)\\&+(4x^4+65x^3+54x^2+19x-28)f'(x)\\&+2(x^4+18x^3+27x^2+22x-6)f(x)=0.\end{aligned}$$

- Let $g(x)$ be the unique power series solution of this differential equation starting like $g(x) = 1 + x + 4x^2 + \frac{65}{6}x^3 + \cdots$.
- Use closure properties to prove that

$$\boxed{2x}\,\boxed{g(x)} + \boxed{e^x(x+1)}\,\boxed{\boxed{g(x)}^2} + \boxed{(2x-1)}\,\boxed{g'(x)} = 0.$$

- Compute the first ≈ 20 terms of $f(x)$ using the given equation.
- Use them to guess the differential equation

$$
\begin{aligned}
&(x+1)(2x-1)(x^2+14x-5)f''(x) \\
&+(4x^4+65x^3+54x^2+19x-28)f'(x) \\
&+2(x^4+18x^3+27x^2+22x-6)f(x)=0.
\end{aligned}
$$

- Let $g(x)$ be the unique power series solution of this differential equation starting like $g(x)=1+x+4x^2+\frac{65}{6}x^3+\cdots$.
- Use closure properties to prove that

$$\boxed{\boxed{2x}\,\boxed{g(x)}}+\boxed{\boxed{e^x(x+1)}\,\boxed{\boxed{g(x)}^2}}+\boxed{\boxed{(2x-1)}\,\boxed{g'(x)}}=0.$$

- Compute the first ≈ 20 terms of $f(x)$ using the given equation.
- Use them to guess the differential equation

$$
\begin{aligned}
&(x+1)(2x-1)(x^2+14x-5)f''(x) \\
&+ (4x^4+65x^3+54x^2+19x-28)f'(x) \\
&+ 2(x^4+18x^3+27x^2+22x-6)f(x) = 0.
\end{aligned}
$$

- Let $g(x)$ be the unique power series solution of this differential equation starting like $g(x) = 1 + x + 4x^2 + \frac{65}{6}x^3 + \cdots$.
- Use closure properties to prove that

$$\boxed{\boxed{\boxed{2x}\,\boxed{g(x)}} + \boxed{\boxed{e^x(x+1)}\,\boxed{\boxed{g(x)}^2}} + \boxed{\boxed{(2x-1)}\,\boxed{g'(x)}}} = 0.$$

- Compute the first ≈ 20 terms of $f(x)$ using the given equation.
- Use them to guess the differential equation

$$\begin{aligned}&(x+1)(2x-1)(x^2+14x-5)f''(x)\\&+(4x^4+65x^3+54x^2+19x-28)f'(x)\\&+2(x^4+18x^3+27x^2+22x-6)f(x)=0.\end{aligned}$$

- Let $g(x)$ be the unique power series solution of this differential equation starting like $g(x) = 1 + x + 4x^2 + \frac{65}{6}x^3 + \cdots$.
- Use closure properties to prove that

$$\boxed{\boxed{\boxed{2x}\,\boxed{g(x)}}+\boxed{\boxed{e^x(x+1)}\,\boxed{\boxed{g(x)}^2}}+\boxed{\boxed{(2x-1)}\,\boxed{g'(x)}}}=0.$$

- Because of uniqueness, we have $f(x) = g(x)$. It follows that $f(x)$ is D-finite.

Lesson 7: Guessing is easy, but proving is not necessarily harder.

f is a D-finite function, i.e., a solution of a linear differential equation

$$p_0(x)f(x) + \cdots + p_r(x)f^{(r)}(x) = 0$$

with polynomial coefficients $p_0, \ldots, p_r$, if and only if the vector space generated by $f, f', f'', \ldots$ over the rational function field has finite dimension:

$$\begin{aligned} &\mathbb{Q}(x)f + \mathbb{Q}(x)f' + \mathbb{Q}(x)f'' + \cdots \\ &= \mathbb{Q}(x)f + \mathbb{Q}(x)f' + \cdots + \mathbb{Q}(x)f^{(r-1)}. \end{aligned}$$

From this characterization, D-finite closure properties are easy to understand.

From this characterization, D-finite closure properties are easy to understand.

Example:

- Suppose f and g are D-finite

From this characterization, D-finite closure properties are easy to understand.

Example:

- Suppose f and g are D-finite
- Then $\dim_{\mathbb{Q}(x)}\langle f, f', \ldots\rangle < \infty$ and $\dim_{\mathbb{Q}(x)}\langle g, g', \ldots\rangle < \infty$

From this characterization, D-finite closure properties are easy to understand.

Example:

- Suppose f and g are D-finite
- Then $\dim_{\mathbb{Q}(x)}\langle f, f', \dots\rangle < \infty$ and $\dim_{\mathbb{Q}(x)}\langle g, g', \dots\rangle < \infty$
- Set $V := \langle f, f', \dots\rangle + \langle g, g', \dots\rangle$. Then $\dim_{\mathbb{Q}(x)} V < \infty$

From this characterization, D-finite closure properties are easy to understand.

Example:

- Suppose f and g are D-finite
- Then $\dim_{\mathbb{Q}(x)}\langle f, f', \dots\rangle < \infty$ and $\dim_{\mathbb{Q}(x)}\langle g, g', \dots\rangle < \infty$
- Set $V := \langle f, f', \dots\rangle + \langle g, g', \dots\rangle$. Then $\dim_{\mathbb{Q}(x)} V < \infty$
- $h := f + g$ and all its derivatives belong to V

From this characterization, D-finite closure properties are easy to understand.

Example:

- Suppose f and g are D-finite
- Then $\dim_{\mathbb{Q}(x)}\langle f, f', \dots\rangle < \infty$ and $\dim_{\mathbb{Q}(x)}\langle g, g', \dots\rangle < \infty$
- Set $V := \langle f, f', \dots\rangle + \langle g, g', \dots\rangle$. Then $\dim_{\mathbb{Q}(x)} V < \infty$
- $h := f + g$ and all its derivatives belong to V
- Hence $h, h', \dots, h^{(r)}$ must be linearly dependent over $\mathbb{Q}(x)$ when r is large enough. So h is D-finite.

From this characterization, D-finite closure properties are easy to understand.

Example:

- Suppose f and g are D-finite
- Then $\dim_{\mathbb{Q}(x)}\langle f, f', \dots\rangle < \infty$ and $\dim_{\mathbb{Q}(x)}\langle g, g', \dots\rangle < \infty$
- Set $V := \langle f, f', \dots\rangle + \langle g, g', \dots\rangle$. Then $\dim_{\mathbb{Q}(x)} V < \infty$
- $h := f + g$ and all its derivatives belong to V
- Hence $h, h', \dots, h^{(r)}$ must be linearly dependent over $\mathbb{Q}(x)$ when r is large enough. So h is D-finite.

This argument, and in fact the whole idea of D-finiteness, extends to a more general setting.

Let us consider operators acting on functions.

$$\underset{\substack{\uparrow\\ \text{operator}\\ \text{algebra}}}{}\cdot : \underset{\substack{\uparrow\\ \text{operator}\\ \text{algebra}}}{A} \times \overset{\substack{\text{function}\\ \text{space}\\ \downarrow}}{F} \longrightarrow F$$

Let us consider operators acting on functions.

$$\underset{\substack{\uparrow\\ \text{operator}\\ \text{algebra}}}{\cdot : A} \times \overset{\substack{\text{function}\\ \text{space}\\ \downarrow}}{F} \longrightarrow F$$

Examples:

- differential operators: $x \cdot (t \mapsto f(t)) := (t \mapsto t\, f(t))$
  $\partial \cdot (t \mapsto f(t)) := (t \mapsto f'(t))$
- recurrence operators: $x \cdot (a_n)_{n=0}^{\infty} := (n\, a_n)_{n=0}^{\infty}$
  $\partial \cdot (a_n)_{n=0}^{\infty} := (a_{n+1})_{n=0}^{\infty}$
- q-recurrence operators: $x \cdot (a_n)_{n=0}^{\infty} := (q^n a_n)_{n=0}^{\infty}$
  $\partial \cdot (a_n)_{n=0}^{\infty} := (a_{n+1})_{n=0}^{\infty}$

Want: Action should be compatible with polynomial arithmetic

$$(L + M) \cdot f = (L \cdot f) + (M \cdot f)$$
$$L \cdot (f + g) = (L \cdot f) + (L \cdot g)$$
$$(LM) \cdot f = L \cdot (M \cdot f)$$
$$1 \cdot f = f$$

Want: Action should be compatible with polynomial arithmetic

$$(L + M) \cdot f = (L \cdot f) + (M \cdot f)$$
$$L \cdot (f + g) = (L \cdot f) + (L \cdot g)$$
$$(LM) \cdot f = L \cdot (M \cdot f)$$
$$1 \cdot f = f$$

Problem: This does not happen automatically.

Want: Action should be compatible with polynomial arithmetic

$$(L + M) \cdot f = (L \cdot f) + (M \cdot f)$$
$$L \cdot (f + g) = (L \cdot f) + (L \cdot g)$$
$$(LM) \cdot f = L \cdot (M \cdot f)$$
$$1 \cdot f = f$$

Problem: This does not happen automatically.

Example: For differential operators, we have

$$(x\partial) \cdot f = x \cdot f' = (t \mapsto t\, f'(t))$$
$$(\partial x) \cdot f = \partial \cdot (t \mapsto t\, f(t)) = (t \mapsto f(t) + t\, f'(t))$$

Want: Action should be compatible with polynomial arithmetic

$$(L + M) \cdot f = (L \cdot f) + (M \cdot f)$$
$$L \cdot (f + g) = (L \cdot f) + (L \cdot g)$$
$$(LM) \cdot f = L \cdot (M \cdot f)$$
$$1 \cdot f = f$$

Problem: This does not happen automatically.

Example: For differential operators, we have

$$(x\partial) \cdot f = x \cdot f' = (t \mapsto t\, f'(t))$$
$$(\partial x) \cdot f = \partial \cdot (t \mapsto t\, f(t)) = (t \mapsto f(t) + t\, f'(t))$$

We need to change multiplication so as to fit to the action.

Definition

Definition

- Let K be a field

Definition

- Let K be a field
- Let $\sigma\colon K \to K$ be an endomorphism, i.e.,

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b)$$

Definition

- Let K be a field
- Let $\sigma\colon K \to K$ be an endomorphism
- Let $\delta\colon K \to K$ be a "σ-derivation", i.e.,

$$\delta(a+b) = \delta(a) + \delta(b) \quad \text{and} \quad \delta(ab) = \delta(a)b + \sigma(a)\delta(b)$$

Definition

- Let K be a field
- Let $\sigma \colon K \to K$ be an endomorphism
- Let $\delta \colon K \to K$ be a "σ-derivation"
- Let $A = K[\partial]$ be the set of all univariate polynomials in ∂ with coefficients in K.

Definition

- Let K be a field
- Let $\sigma\colon \mathrm{K} \to \mathrm{K}$ be an endomorphism
- Let $\delta\colon \mathrm{K} \to \mathrm{K}$ be a "σ-derivation"
- Let $A = \mathrm{K}[\partial]$ be the set of all univariate polynomials in ∂ with coefficients in K.
- Let $+$ be the usual polynomial addition.

Definition

- Let K be a field
- Let $\sigma\colon K \to K$ be an endomorphism
- Let $\delta\colon K \to K$ be a "σ-derivation"
- Let $A = K[\partial]$ be the set of all univariate polynomials in ∂ with coefficients in K.
- Let $+$ be the usual polynomial addition.
- Let $\cdot$ be the unique (noncommutative) multiplication in A which extends the multiplication in R and satisfies

$$\partial a = \sigma(a)\partial + \delta(a) \qquad \text{for all } a \in K.$$

Definition

- Let K be a field
- Let $\sigma \colon K \to K$ be an endomorphism
- Let $\delta \colon K \to K$ be a "σ-derivation"
- Let $A = K[\partial]$ be the set of all univariate polynomials in ∂ with coefficients in K.
- Let $+$ be the usual polynomial addition.
- Let $\cdot$ be the unique (noncommutative) multiplication in A which extends the multiplication in R and satisfies

$$\partial a = \sigma(a)\partial + \delta(a) \qquad \text{for all } a \in K.$$

- Then A together with this $+$ and $\cdot$ is called an Ore Algebra.

Examples: $A = \mathbb{Q}(x)[\partial]$

Examples: $A = \mathbb{Q}(x)[\partial]$

- differential operators: $\sigma = \mathrm{id}$, $\delta = \frac{d}{dx}$

$$\partial x = x\partial + 1$$

Examples: $A = \mathbb{Q}(x)[\partial]$

- differential operators: $\sigma = \mathrm{id}$, $\delta = \frac{d}{dx}$

$$\partial x = x\partial + 1$$

- recurrence operators: $\sigma(p(x)) = p(x+1)$, $\delta = 0$

$$\partial x = (x+1)\partial$$

Examples: $A = \mathbb{Q}(x)[\partial]$

- differential operators: $\sigma = \mathrm{id}$, $\delta = \frac{d}{dx}$

$$\partial x = x\partial + 1$$

- recurrence operators: $\sigma(p(x)) = p(x+1)$, $\delta = 0$

$$\partial x = (x+1)\partial$$

- q-recurrence operators: $\sigma(p(x)) = p(qx)$, $\delta = 0$

$$\partial x = qx\partial$$

Let $A = K[\partial]$ be an Ore algebra acting on a function space F.

Let $A = K[\partial]$ be an Ore algebra acting on a function space F.

- The annihilator of $f \in F$ is defined as

$$\operatorname{ann}(f) := \{\, a \in A : a \cdot f = 0 \,\} \subseteq A.$$

  Its elements are called annihilating operators for f.

Let $A = K[\partial]$ be an Ore algebra acting on a function space F.

- The annihilator of $f \in F$ is defined as

$$\operatorname{ann}(f) := \{\, a \in A : a \cdot f = 0 \,\} \subseteq A.$$

  Its elements are called annihilating operators for f.

- The solution space of $a \in A$ is defined as

$$V(a) := \{\, f \in F : a \cdot f = 0 \,\} \subseteq F.$$

  Its elements are called solutions of a.

Let $A = K[\partial]$ be an Ore algebra acting on a function space F.

- The annihilator of $f \in F$ is defined as

$$\operatorname{ann}(f) := \{\, a \in A : a \cdot f = 0 \,\} \subseteq A.$$

Its elements are called annihilating operators for f.

This is a left-ideal of A.

- The solution space of $a \in A$ is defined as

$$V(a) := \{\, f \in F : a \cdot f = 0 \,\} \subseteq F.$$

Its elements are called solutions of a.

Let $A = K[\partial]$ be an Ore algebra acting on a function space F.

- The annihilator of $f \in F$ is defined as

  $$\operatorname{ann}(f) := \{\, a \in A : a \cdot f = 0 \,\} \subseteq A.$$

  Its elements are called annihilating operators for f.

  This is a left-ideal of A.

- The solution space of $a \in A$ is defined as

  $$V(a) := \{\, f \in F : a \cdot f = 0 \,\} \subseteq F.$$

  Its elements are called solutions of a.

  This is a C-subspace of F, where $C = \{\, c \in K : c\partial = \partial c \,\}$.

Let $A = K[\partial]$ be an Ore algebra acting on a function space F.

- $f \in F$ is called D-finite (w.r.t. the action of A on F) if

$$\operatorname{ann}(f) \neq \{0\}.$$

Let $A = K[\partial]$ be an Ore algebra acting on a function space F.

- $f \in F$ is called D-finite (w.r.t. the action of A on F) if

$$\operatorname{ann}(f) \neq \{0\}.$$

- This is the case if and only if

$$\dim_K K[\partial]/\operatorname{ann}(f) < \infty$$

Let $A = K[\partial]$ be an Ore algebra acting on a function space F.

- $f \in F$ is called D-finite (w.r.t. the action of A on F) if

$$\mathrm{ann}(f) \neq \{0\}.$$

- This is the case if and only if

$$\dim_K K[\underset{\uparrow}{\partial}]/\mathrm{ann}(f) \underbrace{< \infty}_{\uparrow}$$

“D” - “finite”

Let $A = K[\partial]$ be an Ore algebra acting on a function space F.

- $f \in F$ is called D-finite (w.r.t. the action of A on F) if

$$\operatorname{ann}(f) \neq \{0\}.$$

- This is the case if and only if

$$\dim_K \underset{\text{“D”}}{\underset{\uparrow}{K[\partial]}}/\operatorname{ann}(f) \underbrace{< \infty}_{\substack{\uparrow \\ \text{“finite”}}}$$

"D" - "finite"

- Note also:

$$K[\partial]/\operatorname{ann}(f) \cong K[\partial] \cdot f \subseteq F$$

as K-vector spaces.

The setting generalizes to the case of several variables.

The setting generalizes to the case of several variables.

In this case, $A = K[\partial_1, \ldots, \partial_m]$ acts on a function space F.

The setting generalizes to the case of several variables.

In this case, $A = K[\partial_1, \ldots, \partial_m]$ acts on a function space F.

For each ∂_i there is a separate σ_i and δ_i describing its commutation with elements of R.

The setting generalizes to the case of several variables.

In this case, $A = K[\partial_1, \dots, \partial_m]$ acts on a function space F.

For each ∂_i there is a separate σ_i and δ_i describing its commutation with elements of R.

We have $\partial_i \partial_j = \partial_j \partial_i$ for all i, j.

The setting generalizes to the case of several variables.

In this case, $A = K[\partial_1, \dots, \partial_m]$ acts on a function space F.

For each ∂_i there is a separate σ_i and δ_i describing its commutation with elements of R.

We have $\partial_i \partial_j = \partial_j \partial_i$ for all i, j.

Typically, F contains functions in m variables and ∂_i acts nontrivially on the ith variable and does nothing with the others.

The setting generalizes to the case of several variables.

In this case, $A = K[\partial_1, \ldots, \partial_m]$ acts on a function space F.

For each ∂_i there is a separate σ_i and δ_i describing its commutation with elements of R.

We have $\partial_i \partial_j = \partial_j \partial_i$ for all i, j.

Typically, F contains functions in m variables and ∂_i acts nontrivially on the ith variable and does nothing with the others.

Example: $\mathbb{Q}(x, y, z)[D_x, D_y, D_z]$ acts naturally on the space F of meromorphic functions in three variables.

Let $A = K[\partial_1, \dots, \partial_m]$ be an Ore algebra acting on F.

Let $A = K[\partial_1, \ldots, \partial_m]$ be an Ore algebra acting on F.

- The annihilator of $f \in F$ is defined as

$$\operatorname{ann}(f) := \{\, a \in A : a \cdot f = 0 \,\} \subseteq A.$$

  This is a left-ideal of A.

Let $A = K[\partial_1, \ldots, \partial_m]$ be an Ore algebra acting on F.

- The annihilator of $f \in F$ is defined as

$$\operatorname{ann}(f) := \{\, a \in A : a \cdot f = 0 \,\} \subseteq A.$$

  This is a left-ideal of A.

- It remains true that

$$K[\partial_1, \ldots, \partial_m]/\operatorname{ann}(f) \cong K[\partial_1, \ldots, \partial_m] \cdot f \subseteq F$$

  as K-vector spaces.

Let $A = K[\partial_1, \dots, \partial_m]$ be an Ore algebra acting on F.

- The annihilator of $f \in F$ is defined as

$$\operatorname{ann}(f) := \{\, a \in A : a \cdot f = 0 \,\} \subseteq A.$$

  This is a left-ideal of A.

- It remains true that

$$K[\partial_1, \dots, \partial_m]/\operatorname{ann}(f) \cong K[\partial_1, \dots, \partial_m] \cdot f \subseteq F$$

  as K-vector spaces.

- f is called D-finite if

$$\dim_K K[\partial_1, \dots, \partial_m]/\operatorname{ann}(f) < \infty$$

Let $A = K[\partial_1, \dots, \partial_m]$ be an Ore algebra acting on F.

- The annihilator of $f \in F$ is defined as

$$\operatorname{ann}(f) := \{ a \in A : a \cdot f = 0 \} \subseteq A.$$

  This is a left-ideal of A.

- It remains true that

$$K[\partial_1, \dots, \partial_m]/\operatorname{ann}(f) \cong K[\partial_1, \dots, \partial_m] \cdot f \subseteq F$$

  as K-vector spaces.

- f is called D-finite if

$$\dim_K K[\partial_1, \dots, \partial_m]/\operatorname{ann}(f) < \infty$$

- This is the case if and only if $\operatorname{ann}(f) \cap K[\partial_i] \neq \{0\}$ for all i.

Example:

For $f(x, y) = \sqrt{x + y^2} - 3x^2 + y$ and $A = \mathbb{Q}(x, y)[D_x, D_y]$ we have

$$\begin{aligned}\operatorname{ann}(f) = \big\langle &(9x^2 + y + 12xy^2)D_y + (2x + 6x^2y)D_x - (1 + 12xy),\\ &(x + 3x^2y + y^2 + 3xy^3)D_y^2 + (y - 3x^2)D_y - 1\big\rangle.\end{aligned}$$

Example:

For $f(x,y) = \sqrt{x+y^2} - 3x^2 + y$ and $A = \mathbb{Q}(x,y)[D_x, D_y]$ we have

$$\begin{aligned}\operatorname{ann}(f) = \big\langle &(9x^2 + y + 12xy^2)D_y + (2x + 6x^2y)D_x - (1 + 12xy),\\ &(x + 3x^2y + y^2 + 3xy^3)D_y^2 + (y - 3x^2)D_y - 1\big\rangle.\end{aligned}$$

This function is D-finite because

$$\begin{aligned}&\operatorname{ann}(f) \cap \mathbb{Q}(x,y)[D_y]\\ &\quad = \langle (x + 3x^2y + y^2 + 3xy^3)D_y^2 + (y - 3x^2)D_y - 1\rangle \neq \{0\}\\ &\operatorname{ann}(f) \cap \mathbb{Q}(x,y)[D_x]\\ &\quad = \langle 2(x + y^2)(9x^2 + y + 12xy^2)D_x^2 - (27x^2 - y + 48xy^2 + 24y^4)D_x\\ &\qquad\quad + (18x + 12y^2)\rangle \neq \{0\}.\end{aligned}$$

Example:

For $f(n,k) = 2^k + \binom{n}{k}$ and $A = \mathbb{Q}(n,k)[S_n, S_k]$ we have

$$\operatorname{ann}(f) = \langle \bullet + \bullet S_k + \bullet S_n,\\ \bullet + \bullet S_k + \bullet S_k^2 \rangle.$$

Example:

For $f(n,k) = 2^k + \binom{n}{k}$ and $A = \mathbb{Q}(n,k)[S_n, S_k]$ we have

$$\begin{aligned} \operatorname{ann}(f) = \langle & \bullet + \bullet S_k + \bullet S_n, \\ & \bullet + \bullet S_k + \bullet S_k^2 \rangle. \end{aligned}$$

This function is D-finite because

$$\begin{aligned} & \operatorname{ann}(f) \cap \mathbb{Q}(n,k)[S_k] \\ & \quad = \langle \bullet + \bullet S_k + \bullet S_k^2 \rangle \neq \{0\} \\ & \operatorname{ann}(f) \cap \mathbb{Q}(n,k)[S_n] \\ & \quad = \langle -1 - n + (3 - k + 2n) S_n + (-2 + k - n) S_n^2 \rangle \neq \{0\}. \end{aligned}$$

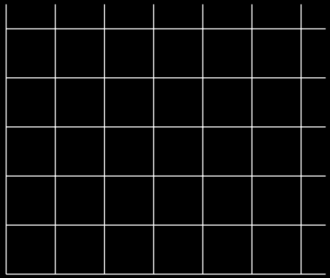
Gröbner bases are also available for ideals in Ore algebras.

Gröbner bases are also available for ideals in Ore algebras.

In particular, a vector space basis of $K[\partial_1, \ldots, \partial_m]/\mathrm{ann}(f)$ is given by the terms $\partial_1^{e_1} \cdots \partial_m^{e_m}$ which are not the leading term of any element of $\mathrm{ann}(f)$.

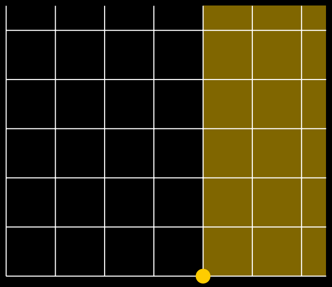
Gröbner bases are also available for ideals in Ore algebras.

In particular, a vector space basis of $K[\partial_1, \ldots, \partial_m]/\operatorname{ann}(f)$ is given by the terms $\partial_1^{e_1} \cdots \partial_m^{e_m}$ which are not the leading term of any element of $\operatorname{ann}(f)$.



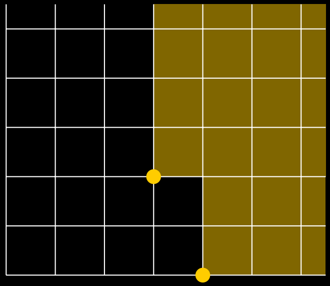
Gröbner bases are also available for ideals in Ore algebras.

In particular, a vector space basis of $K[\partial_1, \ldots, \partial_m]/\mathrm{ann}(f)$ is given by the terms $\partial_1^{e_1} \cdots \partial_m^{e_m}$ which are not the leading term of any element of $\mathrm{ann}(f)$.



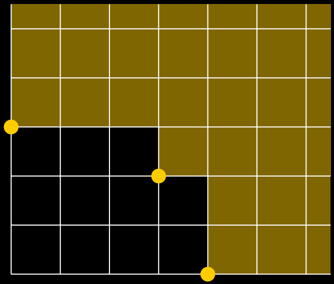
Gröbner bases are also available for ideals in Ore algebras.

In particular, a vector space basis of $K[\partial_1, \ldots, \partial_m]/\operatorname{ann}(f)$ is given by the terms $\partial_1^{e_1} \cdots \partial_m^{e_m}$ which are not the leading term of any element of $\operatorname{ann}(f)$.



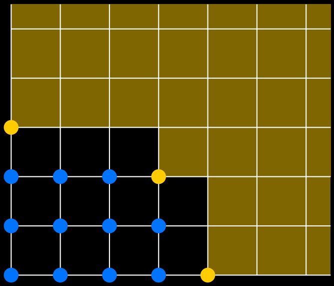
Gröbner bases are also available for ideals in Ore algebras.

In particular, a vector space basis of $K[\partial_1, \dots, \partial_m]/\operatorname{ann}(f)$ is given by the terms $\partial_1^{e_1} \cdots \partial_m^{e_m}$ which are not the leading term of any element of $\operatorname{ann}(f)$.



Gröbner bases are also available for ideals in Ore algebras.

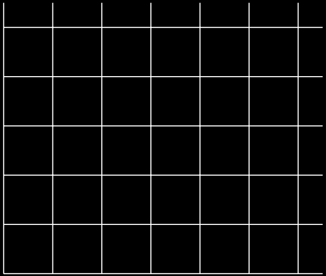
In particular, a vector space basis of $K[\partial_1, \ldots, \partial_m]/\mathrm{ann}(f)$ is given by the terms $\partial_1^{e_1} \cdots \partial_m^{e_m}$ which are not the leading term of any element of $\mathrm{ann}(f)$.



Example:

$f(x, y) = \sqrt{x + y^2} - 3x^2 + y$

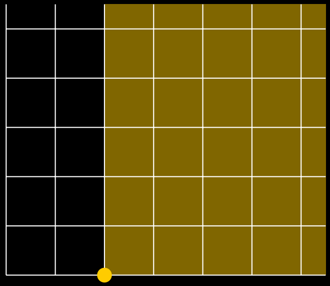
$$\operatorname{ann}(f) = \big\langle (2x + 6x^2 y)\, D_x \; + (9x^2 + y + 12xy^2) D_y - (1 + 12xy),$$
$$(x + 3x^2 y + y^2 + 3xy^3)\, D_y^2 \; + (y - 3x^2) D_y - 1 \big\rangle.$$



Example:

$$f(x,y) = \sqrt{x+y^2} - 3x^2 + y$$

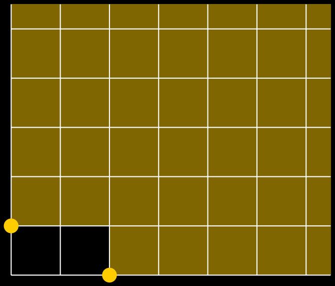
$$\operatorname{ann}(f) = \big\langle (2x+6x^2y)\,D_x + (9x^2+y+12xy^2)D_y - (1+12xy),$$
$$(x+3x^2y+y^2+3xy^3)\boxed{D_y^2} + (y-3x^2)D_y - 1\big\rangle.$$



Example:

$f(x,y) = \sqrt{x+y^2} - 3x^2 + y$

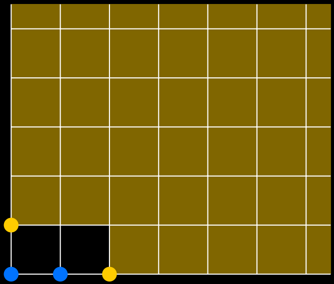
$$\operatorname{ann}(f) = \Big\langle (2x+6x^2y)\boxed{D_x} + (9x^2+y+12xy^2)D_y - (1+12xy),$$
$$(x+3x^2y+y^2+3xy^3)\boxed{D_y^2} + (y-3x^2)D_y - 1\Big\rangle.$$



Example:

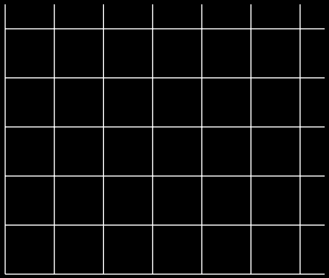
$$f(x,y) = \sqrt{x+y^2} - 3x^2 + y$$

$$\text{ann}(f) = \big\langle (2x+6x^2y)\boxed{D_x} + (9x^2+y+12xy^2)D_y - (1+12xy),$$
$$(x+3x^2y+y^2+3xy^3)\boxed{D_y^2} + (y-3x^2)D_y - 1\big\rangle.$$



Example:
$f_{n,k} = 2^k + \binom{n}{k}$

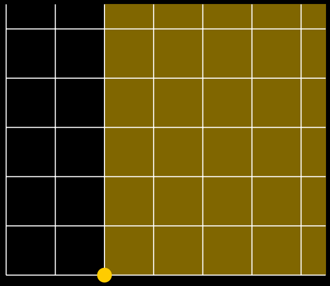
$$\operatorname{ann}(f) = \langle \bullet S_n + \bullet S_k + \bullet,\\ \bullet S_k^2 + \bullet S_k + \bullet \rangle.$$



Example:

$f_{n,k} = 2^k + \binom{n}{k}$

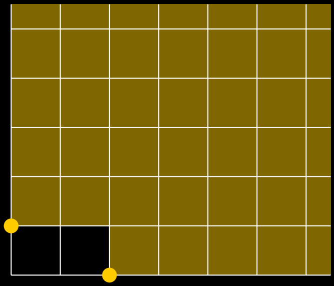
$$\mathrm{ann}(f) = \langle \bullet\, S_n + \bullet\, S_k + \bullet,\\ \bullet\, \boxed{S_k^2} + \bullet\, S_k + \bullet \rangle.$$



Example:

$f_{n,k} = 2^k + \binom{n}{k}$

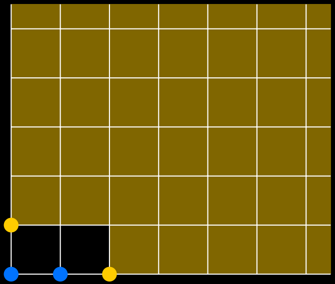
$$\operatorname{ann}(f) = \langle \bullet \boxed{S_n} + \bullet S_k + \bullet,\ \bullet \boxed{S_k^2} + \bullet S_k + \bullet \rangle.$$



Example:

$f_{n,k} = 2^k + \binom{n}{k}$

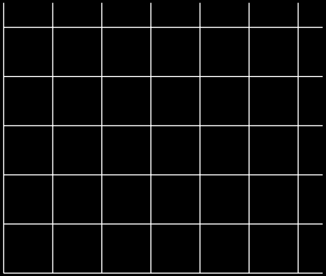
$$\operatorname{ann}(f) = \langle \bullet \boxed{S_n} + \bullet S_k + \bullet, \\ \bullet \boxed{S_k^2} + \bullet S_k + \bullet \rangle.$$



Example:

$P_n(x)$ = the nth Legendre polynomial

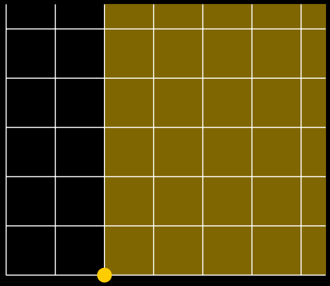
$$\operatorname{ann}(f) = \big\langle (n+1)\, S_n \; + (1-x^2)D_x - (n+1)x,$$
$$(x^2-1)\, D_x^2 \; + 2xD_x - n(n+1) \big\rangle.$$



Example:

$P_n(x)$ = the nth Legendre polynomial

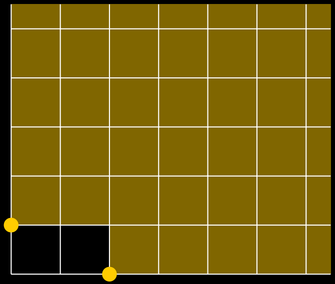
$$\operatorname{ann}(f) = \big\langle (n+1)\,S_n + (1-x^2)D_x - (n+1)x,\\ (x^2-1)\boxed{D_x^2} + 2xD_x - n(n+1)\big\rangle.$$



Example:

$P_n(x)$ = the nth Legendre polynomial

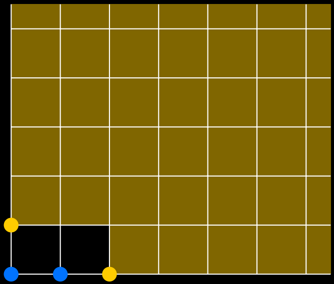
$$\operatorname{ann}(f) = \Big\langle (n+1)\boxed{S_n} + (1-x^2)D_x - (n+1)x,$$
$$(x^2-1)\boxed{D_x^2} + 2xD_x - n(n+1)\Big\rangle.$$



Example:

$P_n(x)$ = the nth Legendre polynomial

$$\operatorname{ann}(f) = \Big\langle (n+1)\boxed{S_n} + (1-x^2)D_x - (n+1)x,$$
$$(x^2-1)\boxed{D_x^2} + 2xD_x - n(n+1)\Big\rangle.$$



Closure properties work as in the univariate case:

- f, g D-finite $\Rightarrow f + g$, fg D-finite
- $f(x, y)$ D-finite and g nonconstant algebraic $\Rightarrow f(x, g)$ D-finite
- $\ldots$

Closure properties work as in the univariate case:

- f, g D-finite $\Rightarrow f + g$, fg D-finite
- $f(x, y)$ D-finite and g nonconstant algebraic $\Rightarrow f(x, g)$ D-finite
- $\ldots$

These properties are realized by linear algebra in $A/\mathrm{ann}(f)$.

Closure properties work as in the univariate case:

- f, g D-finite $\Rightarrow f + g$, fg D-finite
- $f(x, y)$ D-finite and g nonconstant algebraic $\Rightarrow f(x, g)$ D-finite
- $\ldots$

These properties are realized by linear algebra in $A/\mathrm{ann}(f)$.

Additional closure properties (differential case):

Closure properties work as in the univariate case:

- f, g D-finite $\Rightarrow f + g,\ fg$ D-finite
- $f(x, y)$ D-finite and g nonconstant algebraic $\Rightarrow f(x, g)$ D-finite
- $\ldots$

These properties are realized by linear algebra in $A/\mathrm{ann}(f)$.

Additional closure properties (differential case):

- $f(x, t)$ D-finite $\Rightarrow I(x) = \int_0^1 f(x, t)dt$ D-finite

Closure properties work as in the univariate case:

- f, g D-finite $\Rightarrow f + g$, fg D-finite
- $f(x, y)$ D-finite and g nonconstant algebraic $\Rightarrow f(x, g)$ D-finite
- $\ldots$

These properties are realized by linear algebra in $A/\mathrm{ann}(f)$.

Additional closure properties (differential case):

- $f(x, t)$ D-finite $\Rightarrow I(x) = \int_0^1 f(x, t)dt$ D-finite
- $f(x, t)$ D-finite $\Rightarrow C(x) = f(x, 0) = [t^0]f(x, t)$ D-finite

Closure properties work as in the univariate case:

- f, g D-finite $\Rightarrow$ $f + g$, fg D-finite
- $f(x, y)$ D-finite and g nonconstant algebraic $\Rightarrow$ $f(x, g)$ D-finite
- $\ldots$

These properties are realized by linear algebra in $A/\mathrm{ann}(f)$.

Additional closure properties (differential case):

- $f(x, t)$ D-finite $\Rightarrow$ $I(x) = \int_0^1 f(x, t)dt$ D-finite
- $f(x, t)$ D-finite $\Rightarrow$ $C(x) = f(x, 0) = [t^0]f(x, t)$ D-finite
- $f(x, t)$ D-finite $\Rightarrow$ $\Delta(x) = \mathrm{diag}\, f(x, t)$ D-finite

Closure properties work as in the univariate case:

- f, g D-finite $\Rightarrow f + g,\ fg$ D-finite
- $f(x, y)$ D-finite and g nonconstant algebraic $\Rightarrow f(x, g)$ D-finite
- $\ldots$

These properties are realized by linear algebra in $A/\mathrm{ann}(f)$.

Additional closure properties (differential case):

- $f(x, t)$ D-finite $\Rightarrow I(x) = \int_0^1 f(x, t)dt$ D-finite
- $f(x, t)$ D-finite $\Rightarrow C(x) = f(x, 0) = [t^0]f(x, t)$ D-finite
- $f(x, t)$ D-finite $\Rightarrow \Delta(x) = \operatorname{diag} f(x, t)$ D-finite
- $f(x, t)$ D-finite $\Rightarrow P(x, t) = [x^> t^>]f(x, t)$ D-finite

Closure properties work as in the univariate case:

- f, g D-finite $\Rightarrow f + g$, fg D-finite
- $f(x, y)$ D-finite and g nonconstant algebraic $\Rightarrow f(x, g)$ D-finite
- $\dots$

These properties are realized by linear algebra in $A/\mathrm{ann}(f)$.

Additional closure properties (differential case):

- $f(x,t)$ D-finite $\Rightarrow I(x) = \int_0^1 f(x,t)dt$ D-finite
- $f(x,t)$ D-finite $\Rightarrow C(x) = f(x,0) = [t^0]f(x,t)$ D-finite
- $f(x,t)$ D-finite $\Rightarrow \Delta(x) = \operatorname{diag} f(x,t)$ D-finite
- $f(x,t)$ D-finite $\Rightarrow P(x,t) = [x^> t^>]f(x,t)$ D-finite

These properties are realized by creative telescoping.

Lesson 8: We are not limited to one variable and shift or derivation

The functional equation

$$2xf(x) + (x+1)f(x)^2 + (2x-1)f'(x) = 0$$

has a unique power series solution

$$f(x) = 1 + x + \tfrac{7}{2}x^2 + \cdots .$$

The functional equation

$$2xf(x) + (x+1)f(x)^2 + (2x-1)f'(x) = 0$$

has a unique power series solution

$$f(x) = 1 + x + \tfrac{7}{2}x^2 + \cdots .$$

This series does not seem to be D-finite.

The functional equation

$$2xf(x) + (x+1)f(x)^2 + (2x-1)f'(x) = 0$$

has a unique power series solution

$$f(x) = 1 + x + \tfrac{7}{2}x^2 + \cdots .$$

This series does not seem to be D-finite.

But it is differentially algebraic.

Definition.

A power series $f(x)$ is called differentially algebraic (ADE) if there is a nonzero polynomial $p \in \mathbb{Q}[x, y_0, y_1, \ldots, y_r]$ such that

$$p\big(x, f(x), f'(x), \ldots, f^{(r)}(x)\big) = 0.$$

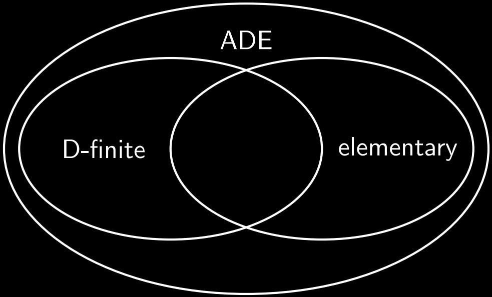
Such an equation is also called an algebraic differential equation.

Definition.

A power series $f(x)$ is called differentially algebraic (ADE) if there is a nonzero polynomial $p \in \mathbb{Q}[x, y_0, y_1, \ldots, y_r]$ such that

$$p\big(x, f(x), f'(x), \ldots, f^{(r)}(x)\big) = 0.$$

Such an equation is also called an algebraic differential equation.



Examples:

- The exponential generating function of the Bell numbers $f(x) = e^{e^x - 1}$ satisfies

$$f(x)f'(x) + f'(x)^2 - f(x)f''(x) = 0.$$

Examples:

- The exponential generating function of the Bell numbers $f(x) = e^{e^x - 1}$ satisfies

$$f(x)f'(x) + f'(x)^2 - f(x)f''(x) = 0.$$

- The exponential generating function of the Bernoulli numbers $f(x) = \frac{x}{e^x - 1}$ satisfies

$$xf'(x) - (1 - x)f(x) + f(x)^2 = 0.$$

Examples:

- The exponential generating function of the Bell numbers $f(x) = e^{e^x - 1}$ satisfies

$$f(x)f'(x) + f'(x)^2 - f(x)f''(x) = 0.$$

- The exponential generating function of the Bernoulli numbers $f(x) = \frac{x}{e^x - 1}$ satisfies

$$xf'(x) - (1 - x)f(x) + f(x)^2 = 0.$$

- The generating function counting the number quarter plane walks with step set $\{\swarrow, \leftarrow, \uparrow, \rightarrow\}$ is differentially algebraic. (The equation is rather big, though.)

The main techniques for D-finite functions can be generalized to ADE functions. In particular:

The main techniques for D-finite functions can be generalized to ADE functions. In particular:

- Guessing: algebraic differential equations can be reconstructed from initial values.

The main techniques for D-finite functions can be generalized to ADE functions. In particular:

- Guessing: algebraic differential equations can be reconstructed from initial values.
  $\longrightarrow$ Ansatz, coefficient comparison, linear system solving.

The main techniques for D-finite functions can be generalized to ADE functions. In particular:

- Guessing: algebraic differential equations can be reconstructed from initial values.
  $\longrightarrow$ Ansatz, coefficient comparison, linear system solving.

- Closure properties: many operations preserve differentially-algebraic-ness.

The main techniques for D-finite functions can be generalized to ADE functions. In particular:

- Guessing: algebraic differential equations can be reconstructed from initial values.
  $\longrightarrow$ Ansatz, coefficient comparison, linear system solving.
- Closure properties: many operations preserve differentially-algebraic-ness.
  $\longrightarrow$ Closure properties can be executed via Gröbner bases.

Example: Let B_n be the Bernoulli numbers defined through

$$f(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

with $xf'(x) - (1-x)f(x) + f(x)^2 = 0$.

Example: Let B_n be the Bernoulli numbers defined through

$$f(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

with $xf'(x) - (1-x)f(x) + f(x)^2 = 0$.

We want to prove the identity

$$\sum_{k=0}^{n} \binom{n}{k} (1 - 2^{1-k})(1 - 2^{1-(n-k)}) B_k B_{n-k} = (1-n) B_n$$

using closure properties.

Example: Let B_n be the Bernoulli numbers defined through

$$f(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

with $x f'(x) - (1-x) f(x) + f(x)^2 = 0$.

We want to prove the identity

$$\sum_{k=0}^{n} \frac{(1-2^{1-k})(1-2^{1-(n-k)}) B_k B_{n-k}}{k!(n-k)!} = \frac{(1-n)}{n!} B_n$$

using closure properties.

Example: Let B_n be the Bernoulli numbers defined through

$$f(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

with $xf'(x) - (1-x)f(x) + f(x)^2 = 0$.

We want to prove the identity

$$\sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{(1-2^{1-k})(1-2^{1-(n-k)}) B_k B_{n-k}}{k!(n-k)!} x^n = \sum_{n=0}^{\infty} \frac{(1-n)}{n!} B_n x^n$$

using closure properties.

Example: Let B_n be the Bernoulli numbers defined through

$$f(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

with $xf'(x) - (1-x)f(x) + f(x)^2 = 0$.

We want to prove the identity

$$\left(\sum_{n=0}^{\infty} (1 - 2^{1-n}) \frac{B_n}{n!} x^n \right)^2 = \sum_{n=0}^{\infty} \frac{(1-n)}{n!} B_n x^n$$

using closure properties.

Example: Let B_n be the Bernoulli numbers defined through

$$f(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

with $xf'(x) - (1-x)f(x) + f(x)^2 = 0$.

We want to prove the identity

$$\big(f(x) - 2f(x/2)\big)^2 = f(x) - xf'(x)$$

using closure properties.

Example: Let B_n be the Bernoulli numbers defined through

$$f(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

with $xf'(x) - (1-x)f(x) + f(x)^2 = 0$.

We want to prove the identity

$$\big(f(x) - 2f(x/2)\big)^2 - f(x) + xf'(x) = 0$$

using closure properties.

Example: Let B_n be the Bernoulli numbers defined through

$$f(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

with $xf'(x) - (1-x)f(x) + f(x)^2 = 0$.

We want to prove the identity

$$h(x) := \big(f(x) - 2f(x/2)\big)^2 - f(x) + xf'(x) = 0$$

using closure properties.

Example: Let B_n be the Bernoulli numbers defined through

$$f(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

with $xf'(x) - (1-x)f(x) + f(x)^2 = 0$.

We want to prove the identity

$$h(x) := \big(f(x) - 2f(x/2)\big)^2 - f(x) + xf'(x) = 0$$

using closure properties.

Compute an ADE for $h(x)$ and check that its unique power series solution starting like $0 + 0x + 0x^2 + \cdots$ is the zero series. ■

$$
\begin{aligned}
&12x^4h(x)^2h''(x)^2 - 12x^2h(x)^4h''(x) + (12x^4 - 16x^2)h(x)^3h''(x) \\
&+ 32x^4h'(x)^4 + 28x^3h(x)^3h'(x) - 96x^3h(x)h'(x)^3 \\
&+ 16x^2h(x)^3h'(x)^2 + (80x^2 - 19x^4)h(x)^2h'(x)^2 \\
&- 16xh(x)^4h'(x) - 40x^4h(x)h'(x)^2h''(x) + 64x^3h(x)^2h'(x)h''(x) \\
&- (6x^2 + 8)h(x)^5 + (3x^4 - 4x^2 - 16)h(x)^4 + 3h(x)^6 = 0.
\end{aligned}
$$

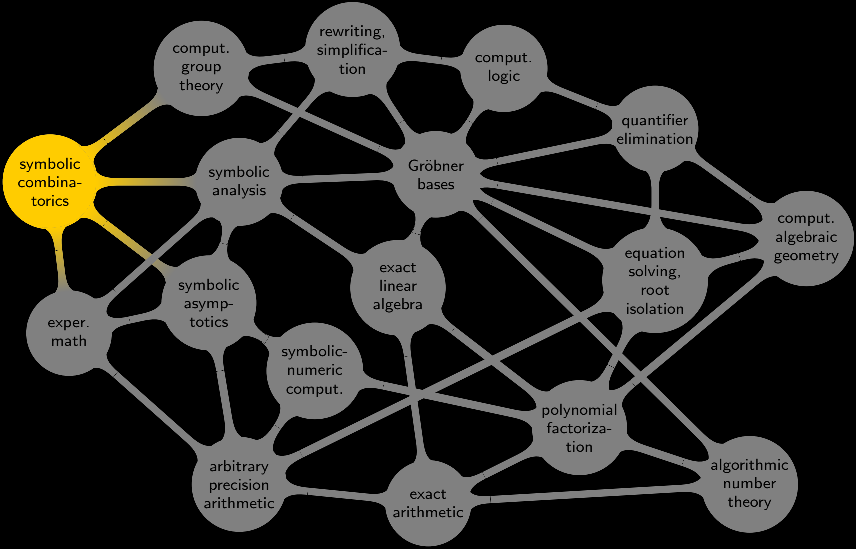
Lesson 9: We are not limited to D-finite functions

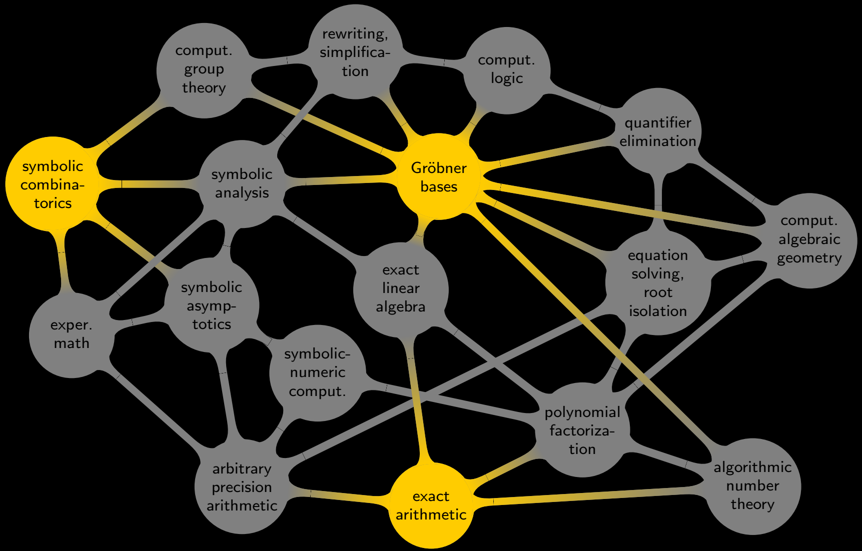
Exercises.

- Find a linear recurrence equation for $\binom{2n}{n} + 2^n - \sum_{k=1}^{n} \frac{1}{1+k^2}$, and a differential equation for its generating function.

- How do we need to define σ and δ in order to obtain an Ore algebra where ∂ acts like $\partial \cdot f(x) = f(x+1) - f(x)$?

- Show that when $f(x)$ is differentially algebraic, then so are $1/f(x)$, $\sqrt{f(x)}$, $\exp(f(x))$, and $\log(f(x))$.


comput. group theory
rewriting, simplifica- tion
comput. logic
quantifier elimination
symbolic combina- torics
symbolic analysis
Gröbner bases
comput. algebraic geometry
equation solving, root isolation
exact linear algebra
symbolic asymp- totics
exper. math
symbolic- numeric comput.
polynomial factoriza- tion
arbitrary precision arithmetic
exact arithmetic
algorithmic number theory


comput. group theory
rewriting, simplifica- tion
comput. logic
quantifier elimination
symbolic combina- torics
symbolic analysis
Gröbner bases
comput. algebraic geometry
equation solving, root isolation
exact linear algebra
symbolic asymp- totics
exper. math
symbolic- numeric comput.
polynomial factoriza- tion
arbitrary precision arithmetic
exact arithmetic
algorithmic number theory

Lesson 1: Fast algorithms are really fast

Lesson 2: Organize your computations well

Lesson 3: Sometimes it's faster to take a detour

Lesson 4: Gröbner bases can not only solve nonlinear systems

Lesson 5: Computing a Gröbner basis is not hopeless

Lesson 6: Gröbner bases are useful

Lesson 7: Guessing is easy, but proving is not necessarily harder

Lesson 8: We are not limited to one variable and shift or derivation

Lesson 9: We are not limited to D-finite functions