Set of Support, Demodulation, and Paramodulation

Fundamental Concepts in Theorem Proving
(In memory of Larry Wos)

Maria Paola Bonacina

Visiting: Computer Science Laboratory, SRI International, Menlo Park, CA, USA
Affiliation: Dipartimento di Informatica, Università degli Studi di Verona
Verona, Italy, EU

Invited talk at the 11th Summer School on Formal Techniques (SSFT)

SRI International and Menlo College, Atherton, California, USA, June 3, 2022

Three fundamental concepts in theorem proving

- The ability of distinguishing assumptions and conjecture
- The ability of replacing equals by equals, and
- The ability of generating equations from equations

Larry Wos (1930–2020)

- BS and MS U. Chicago, PhD UIUC
- MCS Division, Argonne National Laboratory since 1957
- Leader of the theorem-proving research group
- A founder of the Conference on Automated Deduction
- First Editor-in-Chief of the Journal of Automated Reasoning
- Founder of the Association for Automated Reasoning
- First Automated Theorem Proving Prize of the American Mathematical Society (with Steve Winker) in 1982
- First Herbrand Award in 1992

Why Argonne?

- (John) Alan Robinson alternated summer jobs at Argonne and Stanford in 1961-1966
- Initial task at Argonne: an implementation of the Davis-Putnam procedure (1960)
- At Argonne Robinson invented first-order resolution by combining propositional resolution (from the Davis-Putnam procedure) and unification (1962-1964)

Two major research problems

- How to control resolution?
  - Wos et al.: the set of support strategy (1965)
- How to build equality into resolution?
  - Wos et al: the demodulation inference rule (1967)
  - Wos et al: the paramodulation inference rule (1969)
- That opened six decades of research in theorem proving

The theorem-proving problem

- A set H of formulas viewed as assumptions or hypotheses
- A formula φ viewed as conjecture
- Theorem-proving problem: $H \models^? \varphi$
- Equivalently: is $H \cup \{\neg\varphi\}$ unsatisfiable?
- Refutation: $H \cup \{\neg\varphi\} \vdash^? \bot$
- If success, then φ is a theorem of H, or $H \supset \varphi$ is a theorem
- Clausal form: $H \cup \{\neg\varphi\} \leadsto S$ set of clauses
- Form of the problem: $S \vdash^? \Box$ (the empty clause)

At the foundations of computer science

- David Hilbert: Entscheidungsproblem (first-order validity)
- Kurt Gödel: completeness of first-order logic
  (truth and theoremhood correspond)
  Later: Leon Henkin (unsatisfiable iff inconsistent)
- Alan Turing: Turing machine, first undecidable problem (halting), reduction of the Entscheidungsproblem to halting
- Jacques Herbrand: semidecidability of first-order validity

Martin Davis. The Universal Computer–The Road from Leibniz to Turing

What is resolution?

An example in propositional logic:

$$\frac{P \vee Q \quad \neg P \vee R}{Q \vee R}$$

One of the inference rule of the Davis-Putnam procedure

Resolution for first-order logic (FOL)

$$\frac{S \cup \{L_1 \vee C,\ L_2 \vee D\}}{S \cup \{L_1 \vee C,\ L_2 \vee D,\ (C \vee D)\sigma\}} \quad L_1\sigma = \neg L_2\sigma$$

- L_1 and L_2 have opposite sign
- σ is a substitution: it replaces variables with terms
- σ is a unifier: it makes the two sides identical
- σ is the most general unifier (mgu): least commitment
- Resolution is an expansion inference rule
- Expansion inference rules use unification

Example

$$\frac{P(g(z),g(y)) \vee \neg R(z,y) \quad \neg P(x,g(a)) \vee Q(x,g(x))}{\neg R(z,a) \vee Q(g(z),g(g(z)))}$$

where $\sigma = \{x \leftarrow g(z),\ y \leftarrow a\}$ is the mgu

$\sigma' = \{x \leftarrow g(b), y \leftarrow a, z \leftarrow b\}$ is not an mgu

Factoring

$$\frac{S \cup \{L_1 \vee \ldots \vee L_k \vee C\}}{S \cup \{L_1 \vee \ldots \vee L_k \vee C,\ (L_1 \vee C)\sigma\}} \quad L_1\sigma = L_2\sigma = \ldots L_k\sigma$$

- σ is the mgu
- Factoring is an expansion inference rule
- Needed for the completeness of resolution: consider $P(x) \vee P(y)$ and $\neg P(z) \vee \neg P(w)$

Subsumption

$$\frac{S \cup \{C,\ D\}}{S \cup \{C\}} \quad C\sigma \subseteq D$$

- σ is a matching substitution
- Clauses as multisets of literals (ex.: $\{P(a), P(a), Q(b)\}$)
- $P(x) \vee P(y)$ does not subsume $P(z)$
- Prevents a clause from subsuming its factors
- $C\sigma \subseteq D$ and $D\sigma \subseteq C$: variants (retain the oldest)
- Subsumption is a contraction inference rule
- Contraction inference rules use matching

Motivation for the set of support strategy

- Even with subsumption, resolution is too prolific
- Too many irrelevant inferences (do not appear in any proof)
- $H \cup \{\neg\varphi\} \leadsto S$: distinction between H and $\neg\varphi$ forgotten
- Larry Wos was interested in problems from mathematics
- In math problems $H \models^{?} \varphi$ the set H is known to be consistent (e.g., presentation of a theory)
- Then what is the point in expanding H?
  It won't give a contradiction!

The set of support strategy

- $H \rightsquigarrow A$: clausal form of H
- $\neg\varphi \rightsquigarrow SOS$: clausal form of $\neg\varphi$: goal clauses
- SOS is the input set of support
- If H is consistent, so is A: no point in expanding A
- A resolution step must have at least one parent from SOS
- All resolvents are added to SOS: only SOS grows
  (the factors of clauses in A are added to A upfront)
- A goal-sensitive strategy

The given-clause algorithm

- Two lists `sos` and `axioms` initialized with *SOS* and *A*
- Loop until proof found or `sos` empty which means sat
- At every iteration: pick a given-clause *C* from `sos`
- The best according to an evaluation function
  (weight, pick-given ratio)
- Perform all expansion steps between *C* and clauses in `axioms`
- Move *C* from `sos` to `axioms`
- Add all newly generated clauses to `sos`
- No inference whose premises are both in *A*

Motivation for demodulation

- Larry Wos was interested in applying theorem proving to mathematics: equality is everywhere
- Reasoning with equations:
  Replacing equals by equals (Birkhoff theorem)
- Problem: non-termination

Example: non-termination due to a cycle

1. $f(a, b, x) \simeq f(x, x, x)$
2. $g(x, y) \simeq x$
3. $g(x, y) \simeq y\}$

Infinite reduction:
$f(g(a, b), g(a, b), g(a, b)) \rightarrow$
$f(a, g(a, b), g(a, b)) \rightarrow$
$f(a, b, g(a, b)) \rightarrow$
$f(g(a, b), g(a, b), g(a, b)) \rightarrow \ldots\ldots\ldots$

Example: non-termination due to infinite growth

$i(x + y) \simeq (i(i(x)) + y) + y$

Infinite reduction:
$i((i(i(0)) + 1) + 1) \rightarrow$
with matching substitution $\{x \leftarrow i(i(0)) + 1, y \leftarrow 1\}$
$(i(i(i(i(0)) + 1)) + 1) + 1 \rightarrow$
with matching substitution $\{x \leftarrow i(i(0)), y \leftarrow 1\}$
$(i((i(i(i(i(0)))) + 1) + 1) + 1) + 1 \rightarrow$
with matching substitution $\{x \leftarrow i(i(i(i(0)))) + 1, y \leftarrow 1\}$
$(((i(i(i(i(i(i(0)))) + 1)) + 1) + 1) + 1) + 1 \rightarrow \ldots\ldots\ldots$

Solution: a well-founded ordering

- Replace s by t only if t is smaller in a well-founded ordering
- An ordering $\succ$ is well-founded if
  there is no infinite descending chain
  $s_0 \succ s_1 \succ \ldots s_i \succ s_{i+1} \succ \ldots$

Larry Wos' demodulation inference rule (1967)

$$\frac{S \cup \{l \simeq r,\ C[l\sigma]\}}{S \cup \{l \simeq r,\ C[r\sigma]\}} \quad \|C[l\sigma]\| > \|C[r\sigma]\|$$

- $l \simeq r$ is called demodulant or demodulator
- σ is a matching substitution
- $\|C\|$ is the number of symbols in C
- Decreasing the number of symbols is well-founded because the ordering on the natural numbers is well-founded

Problems opened by Larry Wos' demodulation

- What if the number of symbols does not change?
  Ex.: $x + y \simeq y + x$
- What if we wanted to increase the number of symbols?
  Ex.: $x * (y + z) \simeq x * y + x * z$
- Does resolution remain refutationally complete if we add demodulation?

Knuth-Bendix completion procedure (1970)

- Orient equations into rewrite rules:
  $l \simeq r$ becomes $l \rightarrow r$ if $l \succ r$ for $\succ$ a well-founded ordering
- Apply $l \rightarrow r$ to rewrite or reduce $t[l\sigma]$ to $t[r\sigma]$
- Knuth-Bendix ordering (KBO): uses a precedence on symbols and a weight function that generalizes symbol count
- Knuth-Bendix completion takes a set of equations E and produces a canonical rewrite systems:
  $E \models \forall \bar{x}.s \simeq t$ iff there exists a u such that $\hat{s} \stackrel{*}{\rightarrow} u \stackrel{*}{\leftarrow} \hat{t}$
- If an equation in E can be neither simplified, nor deleted ($s \simeq s$), nor oriented, the procedure fails

Reduction ordering

- Well-founded
- Stable: $t \succ u$ implies $t\sigma \succ u\sigma$ for all substitutions σ
- Monotonic: $t \succ u$ implies $c[t] \succ c[u]$ for all contexts c
  - Knuth-Bendix orderings
  - Recursive path orderings [Dershowitz 1982]
  - Lexicographic path orderings [Kamin & Lévy 1980]
- In general these orderings are partial, not total!

Knuth-Bendix completion as theorem proving

- $E \models^? \forall \bar{x}.s \simeq t$
- Negating $\forall \bar{x}.s \simeq t$ yields $\exists \bar{x}.s \not\simeq t$ and hence $\hat{s} \not\simeq \hat{t}$ where $\hat{s}$ is s with all vars replaced by Skolem constants
- Refutationally: $E \cup \{\hat{s} \not\simeq \hat{t}\} \vdash^? \Box$
- Apply Knuth-Bendix completion to E and reduce $\hat{s}$ and $\hat{t}$ whenever possible
- Refutation found if $\hat{s} \xrightarrow{*} u$ and $\hat{t} \xrightarrow{*} u$ so that $u \not\simeq u$ contradicts $x \simeq x$
- Complete unless the procedure fails [Gérard Huet 1981]

Knuth-Bendix completion as inference rules

- State of the derivation: $(E; R)$ where E is a set of equations and R a set of rewrite rules
- A reduction ordering on equational proofs
- An inference rule deriving $(E'; R')$ from $(E; R)$ is proof-reducing
  if for all theorems $s \simeq t$ of $E \cup R$ and
  for all proofs π of $s \simeq t$ in $E \cup R$
  there exists a proof π' of $s \simeq t$ in $E' \cup R'$ such that $\pi \geq \pi'$

[Leo Bachmair et al. 1986] [Leo Bachmair & Nachum Dershowitz 1994]

Inference rules for demodulation in KB completion

The Simplify rule reduces a side of an equation:

$$\frac{(E \cup \{p[l\sigma] \simeq q\}; R \cup \{l \rightarrow r\})}{(E \cup \{p[r\sigma] \simeq q\}; R \cup \{l \rightarrow r\})}$$

where $\simeq$ is symmetric

Inference rules for demodulation in KB completion

The Compose rule reduces the right-hand side of a rewrite rule so that another rewrite rule is produced:

$$\frac{(E; R \cup \{p \rightarrow q[l\sigma], l \rightarrow r\})}{(E; R \cup \{p \rightarrow q[r\sigma],\ l \rightarrow r\})}$$

Inference rules for demodulation in KB completion

The Collapse rule reduces the left-hand side of a rewrite rule, so that an equation is produced:

$$\frac{(E; R \cup \{p[l\sigma] \rightarrow q, l \rightarrow r\})}{(E \cup \{p[r\sigma] \simeq q\}; R \cup \{l \rightarrow r\})} \qquad p[l\sigma] \triangleright l$$

where $\triangleright$ is the strict encompassment ordering on terms

The encompassment ordering

- Encompassment: $t \trianglerighteq s$ if $t = c[s\vartheta]$
- ϑ is a substitution
- Strict: either c is not empty or ϑ is not a variable renaming
- Prevent $l \rightarrow r$ from reducing $p[l\sigma]$ if l and $p[l\sigma]$ are variants: not proof-reducing
- Disallow applying $f(e,y) \simeq y$ to reduce $f(e,x) \simeq x$
  Disallow applying $f(e,y) \simeq y$ to reduce $f(e,x) \simeq h(x)$

Still only a partial solution

- What about equations that cannot be oriented into rewrite rules?

Unfailing or ordered completion (1987)

- It is not necessary to orient equations into rewrite rules
- It suffices to orient the applied instances
- The procedure does not fail
- It produces only a ground canonical rewrite system, but ground canonicity is enough for theorem proving: the target theorem $\hat{s} \not\simeq \hat{t}$ is ground
- State of the derivation: $(E; \hat{s} \not\simeq \hat{t})$
  E: set of equations

[Jieh Hsiang & Michaël Rusinowitch 1987] [Leo Bachmair et al. 1989]

Complete simplification ordering

- Subterm property: $c[t] \succeq t$
- Stable: $t \succ u$ implies $t\sigma \succ u\sigma$ for all substitutions σ
- Monotonic: $t \succ u$ implies $c[t] \succ c[u]$ for all contexts c
- These three properties imply well-founded
- Total on ground terms
  - Knuth-Bendix orderings
  - Recursive path orderings (not all)
  - Lexicographic path orderings

Inference rules for demodulation in completion

Simplification of the target

$$\frac{(E \cup \{l \simeq r\}; \hat{s}[l\sigma] \not\simeq \hat{t})}{(E \cup \{l \simeq r\}; \hat{s}[r\sigma] \not\simeq \hat{t})} \quad l\sigma \succ r\sigma$$

Inference rules for demodulation in completion

Simplification of the presentation

$$\frac{(E \cup \{p[l\sigma] \simeq q,\ l \simeq r\}; \hat{s} \not\simeq \hat{t})}{(E \cup \{p[r\sigma] \simeq q,\ l \simeq r\}; \hat{s} \not\simeq \hat{t})}$$

- $l \simeq r$ is called a simplifier
- $l\sigma \succ r\sigma$
- $p[l\sigma] \triangleright l \ \vee\ q \succ p[r\sigma]$

The side condition for simplification of equations

- $p[l\sigma] \triangleright l \ \vee \ q \succ p[r\sigma]$
- It lets $l \simeq r$ simplify $p[l\sigma] \simeq q$ when $p[l\sigma]$ is a variant of l provided that $q \succ p[r\sigma]$
- Apply $f(e, y) \simeq y$ to simplify $f(e, x) \simeq h(x)$?
  Yes because $h(x) \succ x$
- Apply $f(e, y) \simeq y$ to simplify $f(e, x) \simeq x$?
  No because $x \not\succ y$
- Apply $f(e, x) \simeq h(x)$ to simplify $f(e, y) \simeq y$?
  No because $y \not\succ h(y)$

Example of simplification

1. $f(x) \simeq g(x)$
2. $g(h(y)) \simeq k(y)$
3. $f(h(b)) \not\simeq k(b)$ (target theorem)

- Precedence: $f > g > h > k > b$
- (1) simplifies the target to $g(h(b)) \not\simeq k(b)$ with matching substitution $\sigma = \{x \leftarrow h(b)\}$ since $f(h(b)) \succ g(h(b))$
- (2) simplifies $g(h(b)) \not\simeq k(b)$ to $k(b) \not\simeq k(b)$ with matching substitution $\vartheta = \{y \leftarrow b\}$ since $g(h(b)) \succ k(b)$

Still only a partial solution

- What about demodulation of clauses?
- A key step: from ordering terms to ordering literals

Multiset extension

- Multisets, e.g., $\{P(a), P(a), Q(b)\}$, $\{5, 4, 4, 4, 3, 1, 1\}$
- From $\succ$ to $\succ_{mul}$:
  - $M \succ_{mul} \emptyset$ if $M \neq \emptyset$
  - $M \cup \{a\} \succ_{mul} N \cup \{a\}$ if $M \succ_{mul} N$
  - $M \cup \{a\} \succ_{mul} N \cup \{b\}$ if $a \succ b$ and $M \cup \{a\} \succ_{mul} N$
- $\{5\} \succ_{mul} \{4, 4, 4, 3, 1, 1\}$
- If $\succ$ is well-founded then $\succ_{mul}$ is well-founded

[Nachum Dershowitz & Zohar Manna 1979]

From ordering terms to ordering literals

- Complete or completable reduction ordering (all KBO's, RPO's, LPO's)
- Read a positive literal L as $L \simeq \top$ and $\neg L$ as $L \not\simeq \top$ where $\top$ is a new symbol such that $t \succ \top$ for all terms t
- Equality is the only predicate symbol
- Treat $p \simeq q$ as the multiset $\{p, q\}$ and $p \not\simeq q$ as the multiset $\{p, p, q, q\}$
- Apply the multiset extension of the ordering on terms

[Leo Bachmair & Harald Ganzinger 1994]

A simplification inference rule for clauses

$$\frac{S \cup \{C[l\sigma],\ l \simeq r\}}{S \cup \{C[r\sigma],\ l \simeq r\}} \quad l\sigma \succ r\sigma, \qquad C[l\sigma] \succ (l\sigma \simeq r\sigma)$$

In the superposition calculus $\mathcal{SP}$

The above example revisited

1. $f(x) \simeq g(x)$
2. $g(h(y)) \simeq k(y)$
3. $f(h(b)) \not\simeq k(b)$ (target theorem)

- Precedence: $f > g > h > k > b$
- (1) simplifies the target to $g(h(b)) \not\simeq k(b)$
  with matching substitution $\sigma = \{x \leftarrow h(b)\}$
  since $\{f(h(b)), f(h(b)), k(b), k(b)\} \succ_{mul} \{f(h(b)), g(h(b))\}$
- (2) simplifies $g(h(b)) \not\simeq k(b)$ to $k(b) \not\simeq k(b)$
  with matching substitution $\vartheta = \{y \leftarrow b\}$
  since $\{g(h(b)), g(h(b)), k(b), k(b)\} \succ_{mul} \{g(h(b)), k(b)\}$

Another example

1. $f(x) \simeq b$
2. $f(b) \simeq c$

- Precedence: $b \succ c$
- Simplification of completion allows (1) to simplify (2) to $b \simeq c$ with matching substitution $\sigma = \{x \leftarrow b\}$ because $f(b) \succ b$ and $f(b) \trianglerighteq f(x)$
- But $\{f(b), c\} \succ_{mul} \{f(b), b\}$ does not hold
- Simplification of $\mathcal{SP}$ does not apply
- Encompassment demodulation for $\mathcal{SP}$
  [André Duarte and Konstantin Korovin at IJCAR 2022]

Motivation for paramodulation/superposition

- Once replacement of equals by equals is restricted to be well-founded, it does not suffice for completeness
- We need an inference rule that generates equations from equations

The equality axioms in clausal form

$$x \simeq x \qquad (\textit{Reflexivity})$$

$$x \not\simeq y \vee y \simeq x \qquad (\textit{Symmetry})$$

$$x \not\simeq y \vee y \not\simeq z \vee x \simeq z \qquad (\textit{Transitivity})$$

$$\bigvee_{i=1}^{n} x_i \not\simeq y_i \vee f(\bar{x}) \simeq f(\bar{y}) \qquad (\textit{Function Substitutivity})$$

$$\bigvee_{i=1}^{n} x_i \not\simeq y_i \vee \neg P(\bar{x}) \vee P(\bar{y}) \qquad (\textit{Predicate Substitutivity})$$

Added to the input for resolution: not practical!

Larry Wos' paramodulation inference rule (1969)

$$\frac{S \cup \{l \simeq r \vee C,\ M[t] \vee D\}}{S \cup \{l \simeq r \vee C,\ M[t] \vee D,\ (C \vee M[r] \vee D)\sigma\}} \quad l\sigma = t\sigma$$

- $\simeq$ is symmetric and σ is the mgu of l and t
- C and D are disjunctions of literals
- $l \simeq r \vee C$ is the para-from clause
- $l \simeq r$ is the para-from literal
- $M[t] \vee D$ is the para-into clause
- $M[t]$ is the para-into literal
- $(C \vee M[r] \vee D)\sigma$ is called paramodulant

Problems opened by Larry Wos' paramodulation

- Wos–Robinson conjecture:
  paramodulation is refutationally complete
  without paramodulating into variables and
  without functionally reflexive axioms
  Functionally reflexive axioms: $f(\bar{x}) \simeq f(\bar{x})$ for all function symbols f
- Refutational completeness of resolution and paramodulation in the presence of demodulation and other contraction rules?

Knuth-Bendix completion procedure (1970)

Superposition of rewrite rules

$$\frac{(E; R \cup \{l \rightarrow r,\ p[t] \rightarrow q\})}{(E \cup \{p[r]\sigma \simeq q\sigma\}; R \cup \{l \rightarrow r,\ p[t] \rightarrow q\})} \quad t \notin X,\ l\sigma = t\sigma$$

- σ is the mgu of l and t
- t is not a variable (X is the set of variable symbols)
- $p[r]\sigma \simeq q\sigma$ is called a critical pair

Unfailing or ordered completion (1987)

Superposition of equations

$$\frac{E \cup \{l \simeq r,\ p[t] \simeq q\}}{E \cup \{l \simeq r,\ p[t] \simeq q,\ p[r]\sigma \simeq q\sigma\}} \quad t \notin X,\ l\sigma = t\sigma$$

- $l\sigma \not\preceq r\sigma$
- $p[t]\sigma \not\preceq q\sigma$
- $l \simeq r$ and $p[t] \simeq q$ superpose only if their instances by σ are either orientable ($l\sigma \succ r\sigma$) or uncomparable
- Equivalently: only if $l\sigma$ is strictly maximal in $\{l\sigma, r\sigma\}$ and $p[t]\sigma$ is strictly maximal in $\{p[t]\sigma,\ q\sigma\}$

Example

$$\frac{f(z,e) \simeq z \quad f(I(x,y),y) \simeq x}{I(x,e) \simeq x}$$

- $f(z,e)\sigma = f(I(x,y),y)\sigma$
- $\sigma = \{z \leftarrow I(x,e),\ y \leftarrow e\}$ most general unifier
- $f(I(x,e),e) \succ I(x,e)$ (by the subterm property)
- $f(I(x,e),e) \succ x$ (by the subterm property)
- Superposing two equations yields a peak:
  $I(x,e) \leftarrow f(I(x,e),e) \rightarrow x$

Another challenge

How to obtain an inference system for FOL+= that

- Avoids paramodulating or superposing into variables
- Is restricted by the ordering
- Is refutationally complete also in the presence of contraction (e.g., demodulation, subsumption, tautology deletion)
- Reduces to completion for an input of the form $E \cup \{\hat{s} \not\simeq \hat{t}\}$

Maximal literals

- Clauses as multisets of literals
- Literal L is maximal in clause C if
  $\neg(\exists M \in C.\ M \succ L)$ or equivalently $\forall M \in C.\ L \not\prec M$
  The other literals can only be smaller, equal, or uncomparable
- Literal L is strictly maximal in clause C if
  $\neg(\exists M \in C.\ M \succeq L)$ or equivalently $\forall M \in C.\ L \not\preceq M$
  The other literals can only be smaller or uncomparable

(Ordered) Resolution

$$\frac{S \cup \{L_1 \vee C,\ L_2 \vee D\}}{S \cup \{L_1 \vee C,\ L_2 \vee D,\ (C \vee D)\sigma\}}$$

- $L_1\sigma = \neg L_2\sigma$ (σ mgu)
- $\forall M \in C.\ L_1\sigma \not\preceq M\sigma$ (strictly maximal)
- $\forall M \in D.\ L_2\sigma \not\preceq M\sigma$ (strictly maximal)

Example

$$\frac{P(g(z), g(y)) \vee \neg R(z, y), \;\; \neg P(x, g(a)) \vee Q(x, g(x))}{\neg R(z, a) \vee Q(g(z), g(g(z)))}$$

- $\sigma = \{x \leftarrow g(z), \;\; y \leftarrow a\}$
- Check that $P(g(z), g(a)) \not\preceq \neg R(z, a)$
- Check that $P(g(z), g(a)) \not\preceq Q(g(z), g(g(z)))$
- Allowed with precedence $P > R > Q > g$
- Not allowed with precedence $Q > R > P > g > a$

(Ordered) Factoring

$$\frac{S \cup \{L_1 \vee \ldots \vee L_k \vee C\}}{S \cup \{L_1 \vee \ldots \vee L_k \vee C,\ (L_1 \vee C)\sigma\}}$$

- $L_1\sigma = L_2\sigma = \ldots L_k\sigma$ (σ mgu)
- $\forall M \in C.\ L_1\sigma \not\preceq M\sigma$ (strictly maximal)

Toward (ordered) paramodulation / superposition

- Para-from clause: $l \simeq r \vee C$
- Para-into clause:
  - $M[t] \vee D$
  - $p[t] \simeq q \vee D$
  - $p[t] \not\simeq q \vee D$
- $l\sigma = t\sigma$ (mgu σ)
- The subterm t is not a variable ($t \notin X$)

Four ordering-based conditions

(i) Para-from literal strictly maximal: $\forall Q \in C.\ (l \simeq r)\sigma \not\preceq Q\sigma$

(ii) Left-hand side of para-from literal strictly maximal: $l\sigma \not\preceq r\sigma$

(iii.a) Para-into literal strictly maximal: $\forall Q \in D.\ M[t]\sigma \not\preceq Q\sigma$
$\forall Q \in D.\ (p[t] \simeq q)\sigma \not\preceq Q\sigma$

(iii.b) Or maximal if it is a negated equation:
$\forall Q \in D.\ (p[t] \not\simeq q)\sigma \not\prec Q\sigma$

(iv) Left-hand side of positive equational para-into literal strictly maximal: $p[t]\sigma \not\preceq q\sigma$

(Ordered) paramodulation

$$\frac{S \cup \{l \simeq r \vee C,\ M[t] \vee D\}}{S \cup \{l \simeq r \vee C,\ M[t] \vee D,\ (C \vee M[r] \vee D)\sigma\}} \quad (i)\ (ii)\ (iii.a)$$

The refutational completeness of the Ordered Literal Inference System with (ordered) resolution, (ordered) factoring, and (ordered) paramodulation settled the Wos–Robinson conjecture

[Jieh Hsiang & Michaël Rusinowitch 1991]

The superposition calculus $\mathcal{SP}$

Affords all four ordering-based conditions:

$$\frac{S \cup \{l \simeq r \vee C,\ p[t] \simeq q \vee D\}}{S \cup \{l \simeq r \vee C,\ p[t] \simeq q \vee D,\ (C \vee p[r] \simeq q \vee D)\sigma\}}$$

with (i), (ii), (iii.a), and (iv)

$$\frac{S \cup \{l \simeq r \vee C,\ p[t] \not\simeq q \vee D\}}{S \cup \{l \simeq r \vee C,\ p[t] \not\simeq q \vee D,\ (C \vee p[r] \not\simeq q \vee D)\sigma\}}$$

with (i), (ii), (iii.b), and (iv)
and solved also the problem of generalizing completion to FOL+=
[Leo Bachmair & Harald Ganzinger 1994]

Six decades of research

- From the set of support strategy to the given-clause algorithm (Bill McCune with OTTER and Stephan Schulz with EPROVER)
- From demodulation and paramodulation to the superposition calculus $\mathcal{SP}$ [Leo Bachmair & Harald Ganzinger 1994]
- Still at the heart of contemporary first-order theorem provers
- Extended to higher order theorem proving: λ-superposition [Alex Bentkamp et al. 2021]

References

- Maria Paola Bonacina. Set of support, demodulation, paramodulation: a historical perspective. *Journal of Automated Reasoning*, published online 24 May 2022.
- Michael Beeson, Maria Paola Bonacina, Michael Kinyon, and Geoff Sutcliffe. Larry Wos – Visions of automated reasoning. *Journal of Automated Reasoning*, published online 28 February 2022.

Thank you!