2
Proof Compression

Proofs in logic can become very big and complex. The existing theorem provers and theoretical techniques are tree-oriented. They can only deal with proofs in a tree-structure. Such approach leads some derivations to high complexity.

Recent works [4], [12] have implemented ways to compress logical proofs. Some of these approaches are based on circuit-structures. For these new approaches, there is no known automatic theorem prover. This work presents a graph-oriented generical theorem prover. It can handle the new circuit-oriented systems and the tree-oriented techniques as well.

2.1.
Sequent Calculus SEQ_0

As presented in [12] and [8] cfr. Chapter 5, SEQ_0 is defined bellow. The system is also known as Schütte-Rasiowa-Sikorski-Tait as well as one sided system sequent calculus. It is a form of sequent calculus for propositional logic.

2.1.1.
Syntax

1. Propositional *variables*: $\mathfrak{v}_1, \mathfrak{v}_2, \ldots \mathfrak{v}_i, \ldots$
2. Boolean *connectives*: $\vee, \wedge, \neg$ (binary positive or and and; unary atomic negation).
3. *Literals*: $\mathfrak{v}_i, \neg\mathfrak{v}_i$ (variables and negated variables).
4. *Formulas*: $A, B, \ldots$

   Recursively defined:

   If it is literal, it is formula.

   If F and G are formulas, then $F \vee G$ and $F \wedge G$ are formulas.
5. *General negation*: $\bar{F}$

SEQ_0 extends atomic negation onto arbitrary formulas by familiar De Morgan clauses:

$\overline{\mathfrak{v}_i} \coloneqq \neg\mathfrak{v}_i$

$\overline{\neg\mathfrak{v}_i} \coloneqq \mathfrak{v}_i$

$\overline{F \vee G} \coloneqq \bar{F} \wedge \bar{G}$

$\overline{F \wedge G} \coloneqq \bar{F} \vee \bar{G}$

6. *Sequents*: $\Gamma, \Sigma, \Delta, \ldots | \Gamma = F_1, F_2, \ldots F_k$ (finite list of formulas).

   If the equivalent formula $\hat{\Gamma} \coloneqq F_1 \vee F_2 \vee \ldots F_k$ is valid in propositional logic, then Γ is *valid*.

2.1.2. Axioms and rules

All axioms and rules are exposed modulo permutation of/in sequents.

1. *Axioms*:

$$\Gamma, \mathfrak{v}_i, \neg\mathfrak{v}_i$$

2. *Disjunction rule* **D**:

$$\frac{\Gamma, F, G}{\Gamma, F \vee G}\mathbf{D}$$

3. *Conjunction rule* **C**:

$$\frac{\Gamma, F \qquad \Gamma, G}{\Gamma, F \wedge G}\mathbf{C}$$

$F \vee G$ and $F \wedge G$ are called the *main formula* of **D** and **C** exposed, respectively. Formulas occurring in Γ are called *minor* formulas (more precisely: minor formula-occurrences).

2.1.3. Auxiliary Rules

These rules do not belong to SEQ_0.

1. Cut rule **CUT**:

$$\frac{\Gamma, C \qquad \Gamma, \bar{C}}{\Gamma}\mathbf{CUT}$$

C and $\bar{C}$ are called *cut formulas* of **CUT** exposed; formulas occurring in Γ are called *minor*. **CUT** instances whose cut formulas are literals are called *atomic cuts*.

2. Weakened substitution rule **WS**:

$$\frac{\Gamma}{\theta(\Gamma), \Sigma}\mathbf{WS}$$

For any substitution $\theta: Variables \to Formulas$ and uniquely determined homomorphic extension $\theta: Sequents/Formulas \to Sequents/Formulas$. Σ is optional, when it is not present, the rule is a *substitution*. θ can be such that $\theta(\Gamma) = \Gamma$, in this case, the rule is a *weakening*. If both exceptions occur, it is a *repetition*.

For any rule $\frac{\Delta_1, \Delta_2, \ldots \Delta_k}{\Delta}$ and $i = 1,2, \ldots, k$, Δ_i and Δ are called premise and conclusion, respectively. The pair is abbreviate by $\Delta_i \rightarrowtail \Delta$. The entire rule is designated analogously e.g. by $\begin{matrix}\Delta_1 \\ \Delta_2 \\ \vdots \\ \Delta_k\end{matrix} \rightarrowtail \Delta$.

2.1.4. Tree-structured deductions

Let Γ be any given sequent. A tree-structured deduction δ of Γ is a finite sequent tree whose bottom vertex (called *root*) is Γ, the highest vertices (called *leaves*) are axioms, and except for the leaves, every vertex is the conclusion of an instance of a rule of inference in SEQ_0 whose premises are upper neighbors of the conclusion. If two vertices are in the intersection of two given paths, then so is every vertex that lies between them.

2.1.5. Circuit-structured derivations

Let Γ be any given sequent. A circuit-structured deduction δ of Γ is a finite rooted sequent circuit, i.e. simple directed acyclic graph (DAG), whose vertices are labeled by sequents, Γ being the label of the root, that satisfies all conditions of previous definition; it is understood that premises are sources going to the conclusions. Every tree-structured deduction is a circuit-structured one.

A following piece of circuit-structured deduction from Γ, F, G, H to $\Gamma, \Big(\big(F \vee (G \vee H)\big) \wedge \big((F \vee H) \vee G\big)\Big)$ fails to satisfy the tree intersection property.

$$\dfrac{\dfrac{\dfrac{\Gamma, F, G, H}{\Gamma, F, G \vee H}\mathbf{D}}{\Gamma, F \vee (G \vee H)}\mathbf{D} \qquad \dfrac{\dfrac{\Gamma, F, H, G}{\Gamma, F \vee H, G}\mathbf{D}}{\Gamma, (F \vee H) \vee G}\mathbf{D}}{\Gamma, \Big(\big(F \vee (G \vee H)\big) \wedge \big((F \vee H) \vee G\big)\Big)}\boldsymbol{C}$$

$$\Gamma, F, G, H \overset{\mathbf{D}}{\underset{\mathbf{D}}{\rightarrowtail}} \begin{matrix} \Gamma, F, G \vee H \\ \Gamma, F \vee H, G \end{matrix} \overset{\mathbf{D}}{\rightarrowtail} \begin{matrix} \Gamma, F \vee (G \vee H) \\ \Gamma, (F \vee H) \vee G \end{matrix} \overset{\mathbf{C}}{\rightarrowtail} \Gamma, \Big(\big(F \vee (G \vee H)\big) \wedge \big((F \vee H) \vee G\big)\Big)$$

Γ, F, G, H by disjunction leads to $\Gamma, F, G \vee H$ and $\Gamma, F \vee H, G$. Applying disjunction again leads respectively to $\Gamma, F \vee (G \vee H)$ and $\Gamma, (F \vee H) \vee G$; which are premises to the conjunction rule that leads to the consequent $\Gamma, \Big(\big(F \vee (G \vee H)\big) \wedge \big((F \vee H) \vee G\big)\Big)$.

The two representations are valid. The first one is the default way to visualize the proof. Premises and consequents are separated by a horizontal line where the premises are seen over the line and the consequents are below the line. The last representation is less seen. It represents the proof in a circuit representation. This representation illustrates better the advantage of circuits over trees and the way a circuit is stored in a memory, using a data structure.

In the example, using circuit structured derivation; the sequent Γ, F, G, H is not repeated as it would in a tree-structured proof. Instead, when a rule leads to the same sequent, it short-circuits to it. The use of this short-circuiting per see represents a proof contraction.

The contraction is a general result. It can be accomplished by different implementations. One flavor of implementation might short-circuit the proof while applying the rule and identifying an existing premise. Another approach is the theorem prover that searches the proof after applying the deduction rules.

Circuit-structured weakening rule alone can compress deductions, as shown in the example bellow.

$$\dfrac{\begin{array}{cc}\delta_1 & \delta_2 \\ \Downarrow & \Downarrow \\ \Gamma, F & \dfrac{\Gamma, F, G}{\Gamma, F \vee G}\,\mathbf{C}\end{array}}{\Gamma, F \wedge (F \vee G)}\,\boldsymbol{D}$$

$$\delta_1 \Longrightarrow \Gamma, F \rightarrowtail \quad \Gamma, F, G \quad \begin{array}{c}\rightarrowtail^{\mathbf{D}} \\ \rightarrowtail^{\mathbf{C}}\end{array} \quad \Gamma, F \vee G \rightarrowtail \Gamma, F \wedge (F \vee G)$$

Γ, F, G by weakening leads to Γ, F; which is one of the premises of the conjunction rule applied in the example. The circuit structured weakening makes the path $\Gamma, F \rightarrowtail \Gamma, F, G$ to that same sequent Γ, F of the path $\Gamma, F \rightarrowtail \Gamma, F \wedge (F \vee G)$.

2.1.6. Properties

Let δ be a deduction (these definition holds for both circuit-structured and tree-structured deductions).

1. *Size* $s(\delta)$ is the total number of symbols. The *size of a sequent* is the total number of symbols occurring on it.
2. *Weight* $\mathrm{w}(\delta)$ is the total number of vertices.
3. *Height* $\mathrm{h}(\delta)$ is the maximal path length.
4. *Boolean complexity* of a given formula is 1 + total number of positive connectives (connectives that are not negation ($\neg$)) occurring in it.
5. *Cut degree* $\mathrm{cdg}(\delta)$ is the maximal boolean complexity of cut formulas occurring in δ.

2.1.7. Completeness and admissibility

The following theorems are stated in [12] and are stated here in order to provide self containeress.

Theorem I A given sequent Γ is valid iff any (hence both) of the following two conditions holds.

1. Γ has a tree-structured deduction in SEQ_0.
2. Γ has a circuit-structured deduction in SEQ_0.

In particular, since any formula is a sequent, a given formula F is valid in propositional logic iff it has a tree-structured deduction in SEQ_0 and iff it has a circuit structured deduction in SEQ_0.

Proof 1 is well-known. 2 easily follows from 1.

Theorem II The cut rule is admissible in SEQ_0. That is if Γ,C and $\Gamma, \neg C$ are both tree a/o circuit deducible in SEQ_0, then so is Γ.

Proof This readily follows from previous theorem. It says that Γ,C and $\Gamma, \neg C$ are both deducible in SEQ_0 iff $\left(\hat{\Gamma} \vee C\right) \wedge \left(\hat{\Gamma} \vee \neg C\right)$ is valid in propositional logic. This obviously yelds the result, since $\left(\hat{\Gamma} \vee C\right) \wedge \left(\hat{\Gamma} \vee \neg C\right)$ is logically equivalent to $\hat{\Gamma}$. Q.E.D.

Theorem III The weakened substitution rule is admissible in SEQ_0. That is for any sequent Γ and Σ, any variable substitution θ, if Γ is tree a/o circuit deducible in SEQ_0, then so is $\theta(\Gamma), \Sigma$. Hence extending SEQ_0 by cut rule a/o weakened substitution rule does not extend the set of tree a/o circuit deducible sequents.

Proof Suppose that $\Gamma = F_1, F_2, \ldots F_k$ is deducible in SEQ_0. Hence by Theorem I, $\hat{\Gamma} = F_1 \vee F_2 \vee \ldots F_k$ is valid in propositional logic. Moreover, by definition, validity is preserved under arbitrary assignments of formulas for variables, and hence $\theta(F_1) \vee \theta(F_2) \vee \ldots \theta(F_k)$ is valid as well, and obviously so is weakening $\theta(F_1) \vee \theta(F_2) \vee \ldots \theta(F_k) \vee G_1 \vee G_2 \vee \ldots G_m$, where $\Sigma = G_1 \vee G_2 \vee \ldots G_m$. From this, by Theorem I, we arrive at the required deducibility of $\theta(\Gamma), \Sigma$. Q.E.D.

2.2.
Proof Compression Example

A proof compression example from [12] based on weakening a tree-structured proof into a circuit-structured is presented. The compression is from a proof which size was exponential $(2^{k+1}-1)$ to a proof of linear size $(3(k-2)+5)$. The presented proof is for the equation Γ_{2^k} as follows.

$$\Gamma_n \coloneqq \overline{\mathfrak{v}_1}, \mathfrak{v}_1 \wedge \overline{\mathfrak{v}_2}, \mathfrak{v}_2 \wedge \overline{\mathfrak{v}_3}, \ldots \mathfrak{v}_{n-1} \wedge \overline{\mathfrak{v}_n}, \mathfrak{v}_n$$

Γ_n is obtained from a more intuitive equation. Let:

$$A_2 \coloneqq \mathfrak{v}_1 \rightarrow \mathfrak{v}_2$$
$$A_3 \coloneqq A_2 \wedge (\mathfrak{v}_2 \rightarrow \mathfrak{v}_3)$$
$$\vdots$$
$$A_{n+1} \coloneqq A_n \wedge (\mathfrak{v}_n \rightarrow \mathfrak{v}_{n+1})$$
$$\vdots$$

And:

$$B_1 \coloneqq (\mathfrak{v}_1 \rightarrow \mathfrak{v}_1)$$
$$B_2 \coloneqq A_2 \rightarrow (\mathfrak{v}_1 \rightarrow \mathfrak{v}_2)$$
$$B_3 \coloneqq A_3 \rightarrow (\mathfrak{v}_1 \rightarrow \mathfrak{v}_3)$$
$$\vdots$$
$$B_{n+1} \coloneqq A_{n+1} \rightarrow (\mathfrak{v}_1 \rightarrow \mathfrak{v}_{n+1})$$
$$\vdots$$

It is trivial to understand that B_n is a tautology. Γ_n is the canonical sequent form of B_n. It is easily obtained as follows: $a \rightarrow b$ is substituted by $\bar{a} \vee b$.

$$B_n = \left(\mathfrak{v}_1 \rightarrow \mathfrak{v}_2 \wedge (\mathfrak{v}_2 \rightarrow \mathfrak{v}_3) \wedge \ldots (\mathfrak{v}_{n-1} \rightarrow \mathfrak{v}_n)\right) \rightarrow (\mathfrak{v}_1 \rightarrow \mathfrak{v}_n)$$
$$B_n = \neg(\overline{\mathfrak{v}_1} \vee \mathfrak{v}_2 \wedge \overline{\mathfrak{v}_2} \vee \mathfrak{v}_3 \wedge \ldots \overline{\mathfrak{v}_{n-1}} \vee \mathfrak{v}_n) \vee (\overline{\mathfrak{v}_1} \vee \mathfrak{v}_n)$$

Applying De Morgan:

$$B_n = \mathfrak{v}_1 \wedge \overline{\mathfrak{v}_2} \vee \mathfrak{v}_2 \wedge \overline{\mathfrak{v}_3} \vee \ldots \mathfrak{v}_{n-1} \wedge \overline{\mathfrak{v}_n} \vee \overline{\mathfrak{v}_1} \vee \mathfrak{v}_n$$

Replacing "∨" by ",":

$$B_n = \overline{\mathfrak{v}_1}, \mathfrak{v}_1 \wedge \overline{\mathfrak{v}_2}, \mathfrak{v}_2 \wedge \overline{\mathfrak{v}_3}, \ldots \mathfrak{v}_{n-1} \wedge \overline{\mathfrak{v}_n}, \mathfrak{v}_n = \Gamma_n$$

The comparison is made between deductions in SEQ_0 and in SEQ_0+**WS**. As shown in 2.1, the first is tree-structured and the second is circuit structured. The sizes of the deductions of Γ_{2^k} are $2^{k+1}-1$ in SEQ_0 and $(3(k-2)+5)$ in SEQ_0+**WS**. SEQ_0+**CUT** can compress the proof of Γ_{2^k} to polynomial weight. However, SEQ_0+**WS** provides a linear solution which is cutfree, a much interesting result.

Theorem IV Given $\Gamma_n \coloneqq \overline{\mathfrak{v}_1}, \mathfrak{v}_1 \wedge \overline{\mathfrak{v}_2}, \mathfrak{v}_2 \wedge \overline{\mathfrak{v}_3}, \ldots \mathfrak{v}_{n-1} \wedge \overline{\mathfrak{v}_n}, \mathfrak{v}_n$; $\forall \delta(\Gamma_n) | \delta \in SEQ_0; w(\delta) \geq 2n-1$.

Proof The weight (w) of a proof is, by 2.1.6, the number of vertices in it. $\delta \in SEQ_0$, thus it is tree-structured. Let Σ be any sequent obtained from Γ_n by rewriting arbitrary conjunctions $x \wedge y$ to x or to y.

Clearly any Σ contains at least one pair of literals $\mathfrak{v}_i, \overline{\mathfrak{v}_j}$ and the corresponding chain (possibly empty) of conjunctions of either of these four forms:

$$\mathfrak{v}_i \wedge \overline{\mathfrak{v}_{i+1}}, \ldots \mathfrak{v}_{j-1} \wedge \overline{\mathfrak{v}_j} (i \leq j)$$
$$\mathfrak{v}_i \wedge \overline{\mathfrak{v}_{i-1}}, \ldots \mathfrak{v}_{j+1} \wedge \overline{\mathfrak{v}_j} (i \geq j)$$
$$\mathfrak{v}_j \wedge \overline{\mathfrak{v}_{j+1}}, \ldots \mathfrak{v}_{i-1} \wedge \overline{\mathfrak{v}_i} (i \leq j)$$
$$\mathfrak{v}_j \wedge \overline{\mathfrak{v}_{j-1}}, \ldots \mathfrak{v}_{i+1} \wedge \overline{\mathfrak{v}_i} (i \geq j)$$

Let $k \coloneqq min(1+|i-j|)$; given $\delta' = \delta(\Sigma) \in SEQ_0$. By induction on $h(\delta')$, having arrived at a conjunction $\mathfrak{v}_p \wedge \overline{\mathfrak{v}_q} | p, q \in [i,j] \wedge |p-q| = 1$, it is necessary to split it. Without loss of generality assume $i \leq p < p+1 = q \leq j$. And find:

$$w(\delta') = 1 + [2(1+p-i)-1] + [2(1+j-q)-1]$$
$$w(\delta') = 1 + 2(1+p-i) - 1 + 2(1+j-p-1) - 1$$
$$w(\delta') = 2(1+j-i) - 1$$
$$w(\delta') \geq 2k-1$$

In particular, for $\Sigma = \Gamma_n$, $w(\delta) \geq 2n-1$. Q.E.D.

Corollary Any tree-structured deduction of Γ_{2^k} in SEQ_0 has at least $2^{k+1}-1$ vertices.

Theorem V Given $\Gamma_n \coloneqq \overline{\mathfrak{v}_1}, \mathfrak{v}_1 \wedge \overline{\mathfrak{v}_2}, \mathfrak{v}_2 \wedge \overline{\mathfrak{v}_3}, \ldots \mathfrak{v}_{n-1} \wedge \overline{\mathfrak{v}_n}, \mathfrak{v}_n$; $\exists\delta\left(\Gamma_{2^k}\right)|\delta \in SEQ_0 + \mathbf{WS}$; $w(\delta) = \begin{cases} 2k+1 & \Leftarrow k \leq 2 \\ 3(k-2)+5 & \Leftarrow k > 2 \end{cases}$.

Proof The weight (w) of a proof is, by 2.1.6, the number of vertices in it. $\delta \in SEQ_0 + \mathbf{WS}$, thus it is circuit-structured. If k=1,2; the proof is trivial and tree-structured, the weight is given with no difficulties. For $k > 2$, the deduction must be exhibited:

Given $\theta: Variables \rightarrow Literals$:

$$\theta(\mathfrak{v}_i) \coloneqq \begin{cases} \overline{\mathfrak{v}_{2^{k-1}-i+1}} & \Leftarrow 1 \leq i \leq 2^{k-1} \\ \mathfrak{v}_1 & \Leftarrow i > 2^{k-1} \end{cases}$$

In order to prove $\Gamma_{2^k} = \overline{\mathfrak{v}_1}, \mathfrak{v}_1 \wedge \overline{\mathfrak{v}_2}, \mathfrak{v}_2 \wedge \overline{\mathfrak{v}_3}, \ldots \mathfrak{v}_{2^k-1} \wedge \overline{\mathfrak{v}_{2^k}}, \mathfrak{v}_{2^k}$, the conjunction rule (2.1.2) is the first one applied, leading to:

$$\frac{\Gamma_{2^{k-1}}, \Pi \qquad \Delta, \Gamma^*_{2^{k-1}}}{\Gamma_{2^k}} \mathbf{C}$$

$$\Gamma_{2^{k-1}} = \overline{\mathfrak{v}_1}, \mathfrak{v}_1 \wedge \overline{\mathfrak{v}_2}, \mathfrak{v}_2 \wedge \overline{\mathfrak{v}_3}, \ldots \mathfrak{v}_{2^{k-1}-1} \wedge \overline{\mathfrak{v}_{2^{k-1}}}, \mathfrak{v}_{2^{k-1}}$$

$$\Pi = \mathfrak{v}_{2^{k-1}+1} \wedge \overline{\mathfrak{v}_{2^{k-1}+2}}, \mathfrak{v}_{2^{k-1}+2} \wedge \overline{\mathfrak{v}_{2^{k-1}+3}}, \ldots \mathfrak{v}_{2^{k-1}} \wedge \overline{\mathfrak{v}_{2^k}}, \mathfrak{v}_{2^k}$$

$$\Delta = \overline{\mathfrak{v}_1}, \mathfrak{v}_1 \wedge \overline{\mathfrak{v}_2}, \mathfrak{v}_2 \wedge \overline{\mathfrak{v}_3}, \ldots \mathfrak{v}_{2^{k-1}-1} \wedge \overline{\mathfrak{v}_{2^{k-1}}}$$

$$\Gamma^*_{2^{k-1}} = \overline{\mathfrak{v}_{2^{k-1}+1}}, \mathfrak{v}_{2^{k-1}+1} \wedge \overline{\mathfrak{v}_{2^{k-1}+2}}, \mathfrak{v}_{2^{k-1}+2} \wedge \overline{\mathfrak{v}_{2^{k-1}+3}}, \ldots \mathfrak{v}_{2^{k-1}} \wedge \overline{\mathfrak{v}_{2^k}}, \mathfrak{v}_{2^k}$$

Substituting $\Gamma^*_{2^{k-1}}$ by $\theta\left(\Gamma_{2^{k-1}}\right)$, **WS** rule is applied:

$$\delta' \Longrightarrow \Gamma_{2^{k-1}} \overset{\rightarrowtail}{\underset{\rightarrowtail}{}} \begin{matrix} \Gamma_{2^{k-1}}, \Pi \\ \Delta, \theta\left(\Gamma_{2^{k-1}}\right) \end{matrix} \rightarrowtail \Gamma_{2^k}$$

Let:

$$w(\delta) = f(k) = \begin{cases} 2k+1 & \Leftarrow k \leq 2 \\ 3(k-2)+5 & \Leftarrow k > 2 \end{cases}$$

Supposing $\delta' \in SEQ_0 + \mathbf{WS}$ (a circuit structured deduction of $\Gamma_{2^{k-1}}$) and $w(\delta') = f(k-1)$; leads, by induction on k, to $w(\delta) = f(k-1) + 3 = f(k)$. Q.E.D.

The presented results are not original, come from [12].