The Complexity and Proof Complexity of the Comparator Circuit Value Problem

Stephen Cook

Joint work with Yuval Filmus, Dai Tri Man Lê, and Yuli Ye

Department of Computer Science
University of Toronto
Canada

Limits of Theorem Proving, Rome, September 2012

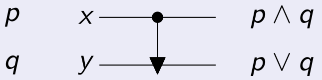
Outline of the talk

1. Define comparator circuits
2. Define CC as the class of problems reducible to $\textsc{Ccv}$ (the comparator circuit value problem)
3. Give interesting complete problems for CC
4. Introduce universal comparator circuits, with resulting robustness properties of CC.
5. Introduce a theory VCC and a propositional proof system CCFrege for CC.
6. Support the conjecture that CC and NC are incomparable using oracle separations.

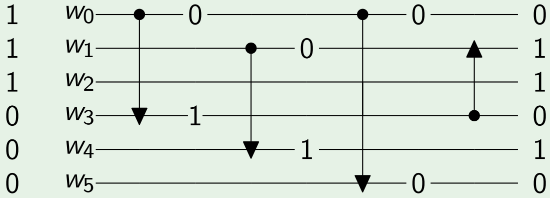
Comparator Circuits

- Originally invented for sorting, e.g.,
  - Batcher's $\mathcal{O}(\log^2 n)$-depth sorting networks ('68)
  - Ajtai-Komlós-Szemerédi (AKS) $\mathcal{O}(\log n)$-depth sorting networks ('83)
- Can also be considered as Boolean circuits.

Comparator gate

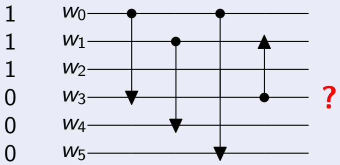


Example



Comparator Circuit Value ($\mathrm{C{\scriptsize CV}}$) Problem (decision)

Given a comparator circuit with specified Boolean inputs, determine the output value of a designated wire.



Comparator Circuit complexity class

1. CC $=$ {decision problems AC^0 many-one-reducible to $\mathrm{C{\scriptsize CV}}$}
2. Subramanian ['90] Defined CC using log space many-one reducibility
3. We introduce universal comparator circuits and use them to show that the two definitions coincide.
4. Subramanian showed

$$\boxed{\mathsf{NL} \subseteq \mathsf{CC} \subseteq \mathsf{P}}$$

NL is nondeterministic log space

- Recall NL $\subseteq$ CC $\subseteq$ P
- But also NL $\subseteq$ NC $\subseteq$ P
  where NC (the parallel class) contains the problems solvable by uniform polysize polylog depth Boolean circuit families.
- NC contains all context-free languages, and matrix powering and determinants over $\mathbb{Z}, \mathbb{Q}$ etc.

Conjecture

NC and CC are incomparable. (So in particular CC $\subsetneq$ P.)

Intuitively, we think CC $\subsetneq$ P because each of the two comparator gate outputs in a comparator circuit is limited to fan-out one. (More later. . .)

Example Complete Problems for CC

- CCV
- Stable Marriage Problem
- Lexicographical first maximal matching
- Telephone connection problem
- Others . . .

Stable Marriage Problem (search version) (Gale-Shapley '62)

- Given n men and n women together with their preference lists
- Find a stable marriage between men and women, i.e.,
  1. a perfect matching
  2. satisfies the stability condition: no two people of the opposite sex like each other more than their current partners
  3. A stable marriage always exists, but may not be unique.

Stable Marriage Problem (decision version)

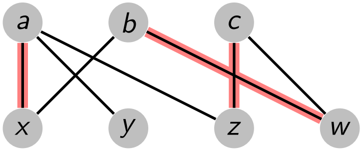
Is a given pair of (m, w) in the man-optimal (woman-optimal) stable marriage?

The Stable Marriage problem has been used to pair medical interns with hospital residencies in the USA.

Lex-first maximal matching problem (CC-Complete)

Lex-first maximal matching

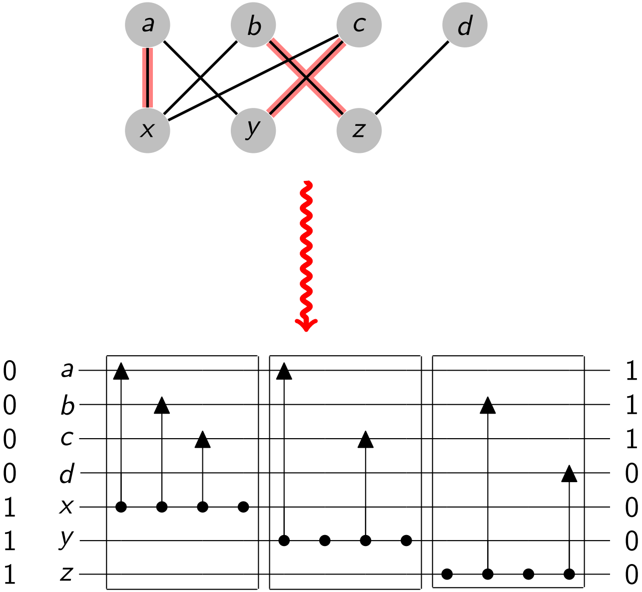
- Let G be a bipartite graph.
- Successively match the bottom nodes $x, y, z, \ldots$ to the least available top node



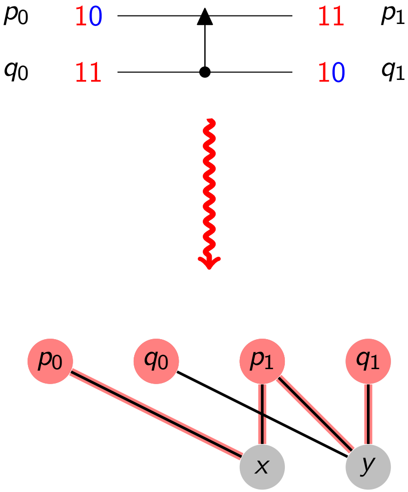
Lex-first maximal matching decision problems

- Edge Is a given edge $\{u, v\}$ in the lex-first maximal matching of G?
- Vertex Is a given (top) vertex v in the lex-first maximal matching of G?
- The problems are equivalent.

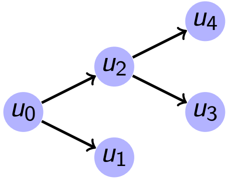
Reducing vertex lex-first maximal matching to $\textsc{Ccv}$



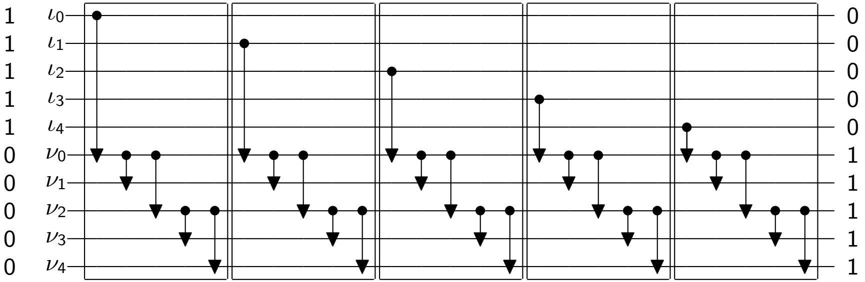
Reducing CCV to lex-first maximal matching



NL $\subseteq$ CC



- This result is due to Feder [1992].
- Dai Lê has a neat proof (See the appendix to our recent arXiv paper.)
- Show $stCONN \leq_m^{AC^0}$ CCV.
- May assume that the given directed graph $G = (V, E)$ has edges of the form (u_i, u_j), where $i < j$.



Two-Sorted Notation

- $x, y, z, \ldots$ denote elements of $\mathbb{N}$ (presented in unary)
- $X, Y, Z, \ldots$ denote binary strings
- $|X|$ denotes the length of X.
- A complexity class is a set of relations of the form $R(\vec{x}, \vec{X})$
- AC^0 many-one reducibility
  $R_1(X) \leq_m^{AC^0} R_2(X)$ iff there exists an AC^0 function $F(X)$ such that

$$R_1(X) \leftrightarrow R_2(F(X))$$

- Thus CC is the class of relations $R(\vec{x}, \vec{X})$ that are AC^0 many-one reducible to $\textsc{Ccv}$.

Function Classes

- Given a class C of relations, we associate a class FC of functions as follows.
- A function F taking strings to strings is in FC iff
  1. $|F(X)| = |X|^{O(1)}$ (p-bounded)
  2. The bit graph $B_F(i, X)$ is in C
- Here $B_F(i, X)$ holds iff the ith bit of $F(X)$ is 1.

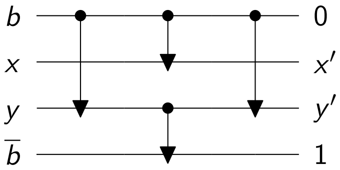
Is FCC closed under composition?

- This question was left open in our earlier paper in CSL 2011 paper (before Yuval Filmus joined our project)
- Suppose $F(X) = G(H(X))$. Let $Y = H(X)$.
- The bit graph of $G(Y)$ is AC^0-reducible to Ccv.
- Thus the circuit computing $G(Y)$ is described by $Y' = \mathsf{AC}^0(Y)$.
- But $Y = H(X)$ is the output of another comparator circuit.

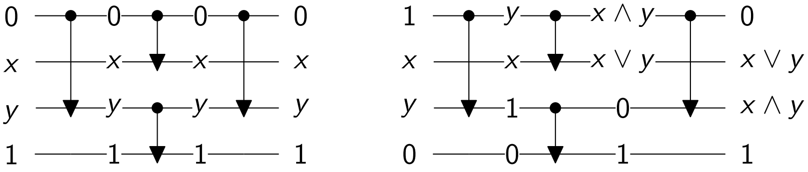
So we need a universal comparator circuit, taking Y' as input, to compute $G(Y)$.

Universal comparator circuits [Filmus]

Here is a gadget which allows a conditional application of a comparator to two of its inputs x, y, depending on whether b is 0 or 1.



Operation of the gadget:



Universal comparator circuits

- In order to simulate a single arbitrary comparator in a circuit with m wires we put in $m(m-1)$ gadgets in a row, for the $m(m-1)$ possible comparators.
- Simulating n comparators requires $m(m-1)n$ gadgets.
- Thus there is an AC^0 function UNIV such that if m, n are arbitrary parameters, then

$$U = \mathrm{UNIV}(m, n) = \langle m', n', U' \rangle$$

is a universal circuit with m' wires and n' gates which simulates all comparator networks with at most m wires and at most n comparators.

$$\begin{aligned} m' &= 2m(m-1)n + m \\ n' &= 4m(m-1)n \end{aligned}$$

Applications of universal comparator circuits

- FCC is closed under composition.
- CC is closed under (many-one) log-space reducibility.
- This is becasue NL $\subseteq$ CC, so FCC includes all log space functions. And FCC is closed under composition.
- If $R(X) \leftrightarrow \mathrm{C{\scriptsize CV}}(F(X))$, where F is log-space computable, then

$$\chi_R(X) = \chi_{\mathrm{C{\scriptsize CV}}}(F(X))$$

where χ_R is the characteristic function of R.

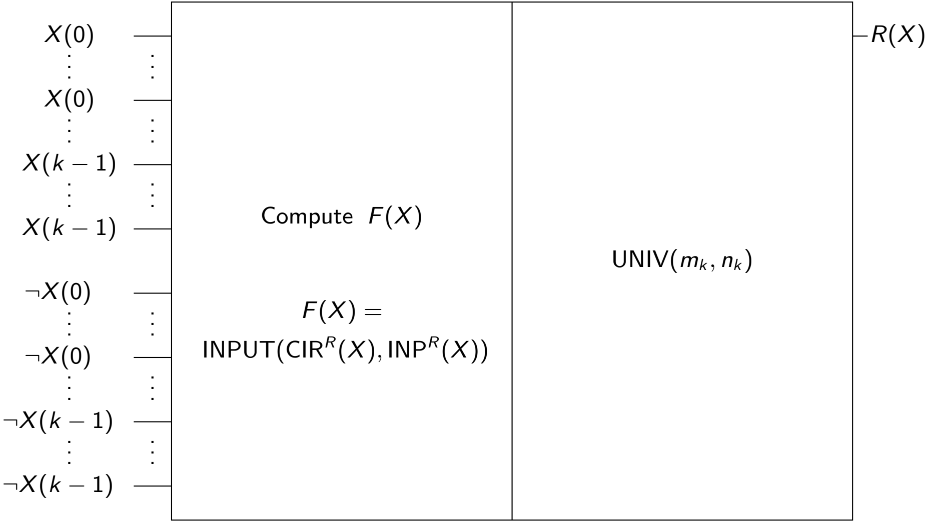
Applications of universal comparator circuits Cont'd

- $R(X)$ is in CC iff there is an AC^0-uniform family $\{C_k^R\}_{k\in\mathbb{N}}$ of comparator circuits, where C_k computes $R(X)$ for $|X| = k$.
- The direction $\Leftarrow$ is immediate.
- Proof of direction $\Rightarrow$: This is clear if $R(X)$ is in AC^0. (An AC^0 circuit converts into a polysize tree circuit, which converts to a comparator circuit.)
- If $R(X) \in \mathrm{CC}$, then

$$R(X) \leftrightarrow \textsc{Ccv}(F(X))$$

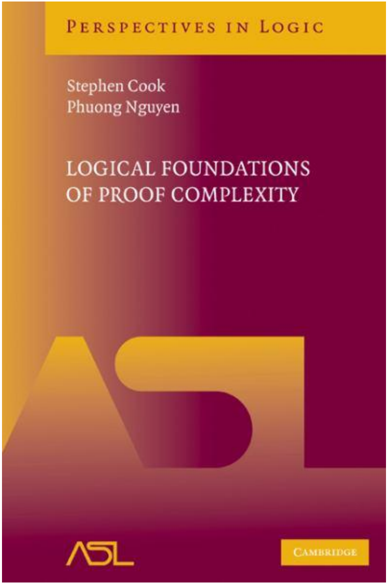
for some AC^0 function $F(X)$. Apply a universal circuit to the output of $F(X)$.

The circuit C_k computing $R(X)$ for $|X| = k$



Theory VCC **for the class** CC

- Reference:



Two-sorted language $\mathcal{L}_A^2$ (Zambella '96)

Vocabulary $\mathcal{L}_A^2 = [0, 1, +, \cdot, |\ |;\ \in, \leq, =_1, =_2]$

- Standard model $\mathbb{N}_2 = \langle \mathbb{N}, \text{finite subsets of } \mathbb{N} \rangle$
- $0, 1, +, \cdot, \leq, =$ have usual meaning over $\mathbb{N}$
- $|X| =$ length of X
- Set membership $y \in X$

Note

The natural inputs for Turing machines and circuits are finite strings.

- "number" variables $x, y, z, \ldots$ (range over $\mathbb{N}$)
- "string" variables $X, Y, Z, \ldots$ (range over finite subsets of $\mathbb{N}$)
- Number terms are built from $x, y, z, \ldots, 0, 1, +, \cdot$ and $|X|, |Y|, |Z|, \ldots$
- The only string terms are variable $X, Y, Z, \ldots$

Definition (Σ_0^B formula)

1. All the number quantifiers are bounded.
2. No string quantifiers (free string variables are allowed)

Two-sorted complexity classes

A two-sorted complexity class consists of relations $R(\vec{x}, \vec{X})$, where

- $\vec{x}$ are number arguments (in unary) and $\vec{X}$ are string arguments

Definition (Two-sorted AC^0)

A relation $R(\vec{x}, \vec{X})$ is in AC^0 iff some alternating Turing machine accepts R in time $\mathcal{O}(\log n)$ with a constant number of alternations.

Σ_0^B-Representation Theorem [from Immerman FO]

$R(\vec{x}, \vec{X})$ is in AC^0 iff it is represented by a Σ_0^B-formula $\varphi(\vec{x}, \vec{X})$.

Useful consequences

1. Don't need to work with uniform circuit families or alternating Turing machines when defining AC^0 functions or relations.
2. Useful when working with AC^0-reductions

The theory V^0 for AC^0 reasoning

Theories developed using Cook-Nguyen method extend V^0.

The axioms of V^0

1. 2-**BASIC axioms**: essentially the axioms of Robinson arithmetic plus
   - the defining axioms for $\leq$ and the string length function $|\ |$
   - the axiom of extensionality for finite sets (bit strings).
2. Σ_0^B-**COMP** (Comprehension): for every Σ_0^B-formula $\varphi(z)$ without X,

$$\exists X \leq y \, \forall z < y \big(X(z) \leftrightarrow \varphi(z) \big)$$

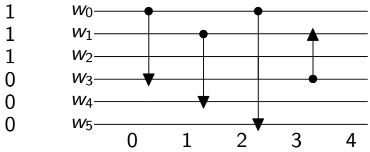
The Σ_0^B-IND scheme is provable in V^0

1. $\big[\varphi(0) \wedge \forall x \big(\varphi(x) \rightarrow \varphi(x+1)\big)\big] \rightarrow \forall x \varphi(x)$, where $\varphi \in \Sigma_0^B$.
2. The provably total functions in V^0 are precisely FAC^0.

The two-sorted theory VCC [using the Cook-Nguyen method]

- VCC has vocabulary $\mathcal{L}_A^2$
- Axiom of VCC $=$ Axiom of V^0 $+$ one additional axiom asserting the existence of a solution to the $\textsc{Ccv}$ problem.

Asserting the existence of a solution to Ccv



- X encodes a comparator circuit with m wires and n gates
- Y encodes the input sequence
- Z is an $(n+1) \times m$ matrix, where column i of Z encodes values layer i

The following Σ_0^B formula $\delta_{\mathsf{CCV}}(m, n, X, Y, Z)$ states that Z encodes the correct values of all the layers of the Ccv instance encoded in X and Y:

$$\forall k < m\big(Y(k) \leftrightarrow Z(0,k)\big) \wedge \forall i < n \forall x < m \forall y < m,$$

$$(X)^i = \langle x, y\rangle \rightarrow \left[\begin{array}{ll} & Z(i+1,x) \leftrightarrow \big(Z(i,x) \wedge Z(i,y)\big) \\ \wedge & Z(i+1,y) \leftrightarrow \big(Z(i,x) \vee Z(i,y)\big) \\ \wedge & \forall j < m\Big[(j \neq x \wedge j \neq y) \rightarrow \big(Z(i+1,j) \leftrightarrow Z(i,j)\big)\Big] \end{array}\right]$$

$$\mathsf{VCC} = \mathsf{V}^0 + \exists Z \leq \langle m, n+1\rangle + 1,\ \delta_{\mathsf{CCV}}(m, n, X, Y, Z)$$

Properties of VCC

From long version of our CSL 2011 paper

- The provably total functions of VCC comprise FCC.
- VCC admits induction on CC concepts.
- VCC extends VNC^1. (Recall $NC^1 \subseteq CC$.)
- VCC proves that Lex-first Max Matching, and Stable Marriage, are complete for CC.

Associate proof system CFrege with VC [Ch. 10, CN 2010]

- Each Σ_0^B formula $\varphi(X)$ translates into a polysize family $\{\varphi(X)[n]\}_{n\in\mathbb{N}}$ of bounded depth propositional formulas.
  - Here $\varphi(X)[n]$ expresses $\varphi(X)$ for $|X| = n$, using atoms p_i^X for the bits of X. (This method due to [Paris/Wilkie]).
- If $\varphi(X)$ is true, then each translated formula $\varphi(X)[n]$ is a tautology.
- If C is a circuit class such as $\mathrm{AC}^0, \mathrm{NC}^1, \mathrm{P}$ then CFrege is AC^0-Frege, Frege, EFrege, respectively.
- The lines in the CFrege-proof represent Boolean circuits of the appropriate kind (bounded-depth, formulas, circuits) respectively.
- A proof of $\varphi(X)$ in the theory VC translates into a polysize family of CFrege proofs of the tautologies $\{\varphi(X)[n]\}_{n\in\mathbb{N}}$
- The theory VC proves the soundness of CFrege.
- CFrege is the strongest proof system whose soundness is provable in VC.

Suggestion for proof system CCFrege

- CCFrege is EFrege with restrictions on introduction of extension variables.
- Each extension variable is the value of some wire segment in a comparator circuit whose inputs do not involve extension variables.
- The extension variables are $w_{ij}, 1 \leq i \leq m, 1 \leq j \leq n$, where the comparator circuit has m wires and n gates.
- w_{ij} is the value of the jth segment of wire i, where each wire gets a new segment after *every* gate.
- Let a_j be the wire number corresponding to the AND of gate j, and let o_j be the wire number corresponding to the OR of gate j.
  Thus $a_j \neq o_j$, and $0 \leq a_j, o_j \leq m$

Defining formulas for the extension variables w_{ij}

- $w_{i0} \leftrightarrow A_i$, $1 \leq i \leq m$, where A_i has no extension variables.
- $w_{i,j+1} \leftrightarrow w_{ij}$ if $i \neq a_j, i \neq o_j$
- $w_{i,j+1} \leftrightarrow (w_{ij} \wedge w_{o_j,j})$ if $i = a_j$
- $w_{i,j+1} \leftrightarrow (w_{ij} \vee w_{a_j,j})$ if $i = o_j$

Properties of CCFrege

Claim:

CCFrege corresponds to VCC:

1. A proof of a Σ_0^B-formula $\varphi(X)$ in the theory VCC translates into a polysize family of CCFrege proofs of the tautologies $\{\varphi(X)[n]\}_{n\in\mathbb{N}}$
2. The theory VCC proves the soundness of CCFrege.
3. CCFrege is the strongest proof system whose soundness is provable in VCC.

Proof of (2)

- Given a CCFrege proof, VCC can evaluate the extension variables in terms of the values for the input variables, using its axiom asserting the existence of values for the wires of a comparator circuit.
- VCC proves by induction that all formulas in the proof are true.

Conjecture: NC and CC are incomparable

- Lex-First Max Matching (LFMM) is in CC.

Conjecture

LFMM is not in NC.
(The obvious algorithm for LFMM is sequential.)

- The function $A \rightsquigarrow A^n$ (where A is an $n \times n$ integer matrix) is in NC^2 , but we do not know how to put it in CC.

Why do we think $\mathsf{NC}^2 \subsetneq \mathsf{CC}$?

- NC^2-gates have multiple fan-out, but each end of a comparator gate has fan-out one.
- If either input of a comparator gate is 'flipped', then exactly one output is flipped.
  Thus comparator gates are 1-Lipschitz.
- Flipping an input to a gate generates a unique flip-path in the circuit from that gate to some output of the circuit.
- But flipping an input to an NC^2-gate can generate many parallel flip-paths.

Relativized CC and NC are incomparable

Oracle gates for comparator circuits

- The oracle $\alpha : \{0,1\}^* \to \{0,1\}^*$ is length preserving.
- $\alpha_n : \{0,1\}^n \to \{0,1\}^n$ is the restriction of α to n.
- An oracle gate α_n can be inserted anywhere in a relativized comparator circuit: select any n wires as inputs to the gate and any n wires as outputs.
- To make α_n gates look more like comparator gates, we require that α_n have the 1-Lipschitz property.
- We allow $\neg$ gates in relativized CC(α) circuits.
(We can allow them in comparator circuits without changing CC.)
- Changing one input to one α_n gate produces a unique flip path in the circuit from that gate to the outputs of the circuit.

Theorem

There is a relation $R_1(\alpha)$ computable by a polysize family of comparator oracle circuits by which cannot be computed by any $\mathsf{NC}(\alpha)$ *circuit family (even when α is restricted to be 1-Lipschitz).*

Proof Idea.

- $\alpha_n^k(\vec{0})$ is easily computed by relativized comparator circuits, but requires depth k circuits [ACN 07].
- The hard part is proving the depth lower bound when α is 1-Lipschitz.

$\square$

Theorem

There is a relation $R_2(\alpha)$ computable by an $\mathsf{NC}^2(\alpha)$ circuit family but not computable by any polysize family of comparator oracle circuits (even when α is restricted to be 1-Lipschitz).

Proof Idea.

- Let $\alpha_i^k : \{0,1\}^{dn} \to \{0,1\}$ be a Boolean oracle.
- Define a function $y = f[(\alpha_1^1, \ldots, \alpha_n^1), \ldots, (\alpha_1^m, \ldots, \alpha_n^m)]$ as follows:

$$\begin{aligned} x_i^k &= \alpha_i^k(\overbrace{x_1^{k+1}, \ldots, x_1^{k+1}}^{d \text{ times}}, \ldots, \overbrace{x_n^{k+1}, \ldots, x_n^{k+1}}^{d \text{ times}}), && k \in [m], i \in [n], \\ x_i^{m+1} &= 0, && i \in [n], \\ y &= x_1^1 \oplus \cdots \oplus x_n^1. \end{aligned}$$

$\square$

Conclusion

The complexity class CC is interesting because

- It is robust (closed under a variety of reductions).
- It has interesting complete problems.
- It appears to be a proper subset of P and incomparable with NC (and SC).
- It has a theory VCC which captures reasoning in CC and proves basic properties of CC.
- It has an associated propositional proof system CCFrege.