Bounded Arithmetic, Constant Depth Proofs, and st-Connectivity

Sam Buss
Department of Mathematics
U.C. San Diego

VIG
Los Angeles
February 2005

Bounded Arithmetic

Theories S_2^i and T_2^i have very close connections to the polynomial time hierarchy.

- Σ_1^b-definable functions of S_2^1 are the polynomial time functions. [B]
- Σ_1^b-definable functions of T_2^1 are the PLS (polynomial local search) functions. [BK]
- For $i > 1$, S_2^i and T_2^i define the $P^{\Sigma_{i-1}^p}$-functions and $PLS^{\Sigma_{i-1}^p}$ functions.

These theories are defined by using hierarchies of bounded formulas, Σ_i^b- and Π_i^b-formulas, defined by counting alternations of bounded quantifiers $(Qx \leq t)$, ignoring sharply bounded quantifiers $(Qx \leq |t|)$. They capture the complexity classes Σ_i^p of the polynomial time hierarchy.

Σ_i^b-PIND induction axioms. For S_2^i:

$$A(0) \wedge (\forall x)(A(\lfloor \tfrac{1}{2}x \rfloor) \rightarrow A(x)) \rightarrow (\forall x)A(x).$$

Σ_i^b-IND induction axioms. For T_2^i:

$$A(0) \wedge (\forall x)(A(x) \rightarrow A(x+1)) \rightarrow (\forall x)A(x).$$

Bounded Arithmetic theories can prove many "simple" polynomial facts and even some stronger items:

Thm [PWW, MPW]. $T_2^2(\alpha) \vdash PHP_x^{2x}(\alpha)$.
(The "2n to n" pigeonhole principle.)

Thm [PWW]. T_2^2 proves that there exists arbitrarily large primes.

On the other hand:

Thm [Krajíček]. $S_2^2(\alpha) \nvdash PHP_x^{2x}(\alpha)$.

Pf idea: Suppose not. There would be a P^{NP} algorithm for finding a violation of the $2x/x$ pigeonhole principle. For each query, if it is possible to obtain a positive answer, set polynomially many ($= (\log x)^c$ many) values of α as a 1-1 function to force the positive answer. Otherwise, return the negative answer. When done, there would be only polynomially many values of α set with α a 1-1 function. This contradicts the existence of the algorithm.

Let $f(x) = (\log x)^{\omega(1)}$. Then, $S_2^2(\alpha) \nvdash PHP_{f(x)}^{g(x)}(\alpha)$, for arbitrary function $g(x)$.

Independence of P vs NP?

There are a couple ways to formalize whether bounded arithmetic can prove $P = NP$, or the collapse of the polynomial hierarchy ($PH \downarrow$).

(1). Does S_2 prove each bounded formula is expressible in Σ_i^b, for some fixed i? Notation: $S_2 \vdash (PH \downarrow)$

Thm.
(a) [KPT] If $S_2^i \prec_{\Sigma_i^b} T_2^i$ then $PH \downarrow$.
(b) [B,Z] $S_2 \vdash (PH \downarrow)$ iff $S_2 \downarrow$.

Notation: $S_2 \downarrow$ means S_2 is finitely axiomatized, or equivalently, that the hierarchy S_2^i collapses.

Unfortunately we have no idea how to show $\neg(S_2 \downarrow)$. If we *could*, this would say something about the logical difficulty of proving $P \neq NP$.

(2) Another approach: Show S_2 cannot prove super-polynomial lower bounds on circuit size....

Thm [Razborov] Fix any polynomial hierarchy predicate $A(x)$. Assume that a strong pseudo-random number generator (SPRNG) conjecture holds. Then $S_2^2(\alpha)$ cannot prove any superpolynomial lower bound on the size of a circuit for $A(x)$.

The predicate α serves to encode a circuit for $A(x)$. Note $S_2^2(\alpha)$ can use IND induction on the size of the circuit, but not its Gödel number.

Proof idea was to the use conservativity of $S_2^2(\alpha)$ over $T_2^1(\alpha)$, witnessing in PLS, interpolation, and then natural proof independence of Razborov-Ruditch which depends on SPRNG.

Thm [BP] The above holds without assuming SPRNG.

Proof idea: Take a natural exponential size circuit for $A(x)$, say a CNF circuit. Let α encode a 1-1, onto violation of the PHP. Using α map exponentially many subcircuits to a set of barely superpolynomial size. Result is a superpolynomial size circuit.
[This proof idea first used by Razborov to prove the independence of superpolynomial circuit size from resolution.]

Constant-Depth Frege Proofs

Def'n: A Frege proof system is a schematic **propositional** proof system. We use a Tait style system; literals are x_i and $\overline{x_i}$ and connectives are unbounded fanin $\wedge$ and $\vee$.

The depth of a formula is the maximum number of alternations of $\wedge$'s and $\vee$'s. This defines classes Π_d and Σ_d of formulas. A depth d proof is a proof in which all formulas are in $\Pi_d \cup \Sigma_d$.

Def'n: Let P be a proof system, Γ a set of formulas and A a formula. Then a P-proof of A from Γ is defined as usual. A P-refutation of Γ is a P-proof of a contradiction from Γ.

Def'n: The *size* of a proof is the number of symbols occurring in the proof.

We are interested in upper and lower bounds on the size of proofs, but usually only up to polynomial factors.

Open: Do all tautologies have polynomial size proofs? If so, then NP is closed under complementation.

Connections to Bounded Arithmetic

Def'n: [Krajíček] A Σ-depth d formula is a Boolean formula of depth $d+1$ where the bottommost gates have (only) logarithmic fanin.

Def'n: Let α be a new predicate symbol. Let $A(x)$ be a $\Sigma^b_d(\alpha)$-formula. Then, $[\![A]\!]$ is a family of polynomial-size Σ-depth d formulas, expressing the condition $\forall x A(x)$. Free variables p_k in the formulas represent the truth values of the predicate $\alpha(k)$. Quantifiers are changed into unbounded $\vee$'s and $\wedge$'s.

Thm: [following Paris-Wilkie] If $T^i_2(\alpha) \vdash \forall x A(x)$ where $A \in \Sigma^b_i$, then $[\![A]\!]$ has quasi-polynomial size Σ-depth i Frege proofs.

Proof idea: Put all formulas into a normal form with sharply bounded quantifiers applied only to open Δ_0 formulas. By cut elimination there is a free-cut free proof. Then transform quantifiers into unbounded fanin boolean connectives.

Thm: [Krajíček'94]. There are sets of depth d formulas which have polynomial size Σ-depth $d+1$ Frege refutations, but require (near) exponential size Σ-depth d Frege refutations.

Open problem: Is there a better separation of (Σ-)depth d and (Σ-)depth $d+1$ Frege proofs?
Are there sets of clauses (Π_2-formulas) which have polynomial size, depth $d+1$ Frege refutations, but require superpolynomial size, depth d Frege refutations? Or Π_i-formulas, for $i \leq d$? (Also open for Σ-depth.)

Uniform version of open problem: For $i \leq j < k$, is $T_2^k(\alpha)$ conservative over $T_2^j(\alpha)$ with respect to $\Sigma_i^b(\alpha)$-formulas?

The good news is that there are superpolynomial lower bounds for constant-depth Frege proofs. The first such exponential lower bound was for the pigeonhole principle:

Def'n: Fix $n > 0$. The negation of the PHP tautology is expressed by the following set of clauses:

$$\{p_{i,j} : 0 \leq j < n\}, \qquad 0 \leq i \leq i$$

$$\{\overline{p}_{i,j}, \overline{p}_{m,j}\}, \quad 0 \leq i < m \leq n, \ 0 \leq j < n.$$

Note that PHP is a set of depth 1 formulas.

Thm: [PBI-KPW'91,93,95]. Depth d refutations of the PHP clauses require size $\Omega(2^{n^{c^{1/d}}})$.

The proof was quite intricate, incorporating an extension of the Hastad switching lemma.

Thm: [B'86] PHP has polynomial size proofs in unrestricted depth propositional systems.

An st-Connectivity Principle

Let G be a directed graph. Let vertex $s \in G$ have out-degree 1 and in-degree zero, and vertex $t \in G$ have in-degree 1 and out-degree 0. Let every other vertex have in-degree 1 and out-degree 1.

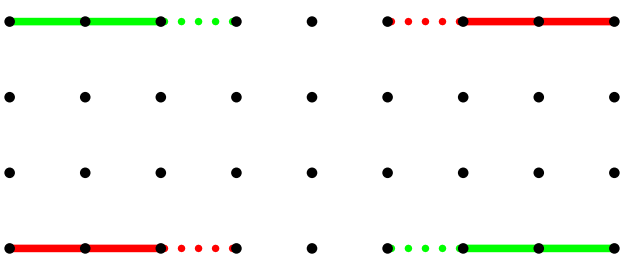
Thm: There is a directed path from s to t.

To avoid the use of the "second-order" concept of a path, we reformulate as follows:

Graph SINK principle: The following is inconsistent:
G is a directed graph in which
- one vertex s has outdegree 1 and indegree 0, and
- every other vertex has both out-degree and in-degree equal to one.

Planar bichromatic connectivity principle

Def'n: A grid graph has vertices (i, j) for $1 \leq i \leq d$ and $1 \leq j \leq n$. Its edges only join vertices which are horizontally or vertically adjacent. Edges can be colored red or green.



Thm: The following conditions are impossible (inconsistent): No vertex has both green and red edges incident. The bottom left and top right vertices each have one red edge incident. The top left and bottom right vertices each have one green edge incident. All other vertices have degree zero or two.

The above is called the **STCONN** principle.

Bounded Depth Circuits for Bounded Width st-Connectivity

Def'n: The depth of a Boolean circuit (or, formula) is the number of alternations of AND's and OR's in the circuit. To measure depth, all negations are pushed to the literals, and AND's and OR's have unbounded fanin. A pure disjunction or conjunction of literals has depth equal to one.

Π_d and Σ_d are the circuit classes of depth d with topmost connective an AND (resp, an OR).

Thm: [Barrington, Lu, Miltersen, Skyjm '98] Given directed graph G of width d and given two vertices s and t, determining if there is a path from s to t is Π_d-complete.

Natural Conjecture [Segerlind]. For $c < d < e$, the width d st-connectivity principles might require large proofs in Π_c-Frege proof systems, but have short (polynomial size) proofs in Π_e-Frege proof systems.

Unfortunately, this turns out to be false.

Constant Depth Proof Reducibilities

Def'n: Let $\mathcal{F}$ be a Frege system. Let S and T be infinite families of tautologies. Let $\mathcal{F}+S$ be $\mathcal{F}$ plus all instances of the S-tautologies. Then $T \preccurlyeq_{cd\mathcal{F}} S$ means that the tautologies T have constant-depth polynomial size proofs in the system $\mathcal{F}+S$.

$S \equiv_{cd\mathcal{F}} T$ means $S \preccurlyeq_{cd\mathcal{F}} T$ and $T \preccurlyeq_{cd\mathcal{F}} S$.

We shall prove:

Thm: [B]

$$\textbf{PHP} \equiv_{cd\mathcal{F}} \textbf{HEX} \equiv_{cd\mathcal{F}} \textbf{SINK} \equiv_{cd\mathcal{F}} \textbf{2SINK} \preccurlyeq_{cd\mathcal{F}} \textbf{DSTCONN} \equiv_{cd\mathcal{F}} \textbf{2DSTCONN} \preccurlyeq_{cd\mathcal{F}} \textbf{STCONN}$$

and

$$\textbf{SINK} \preccurlyeq_{cd\mathcal{F}} \textbf{Mod}_2 \equiv_{cd\mathcal{F}} \textbf{USINK} \preccurlyeq_{cd\mathcal{F}} \textbf{STCONN}.$$

Where **DSTCONN** is a directed version of **STCONN**, and **USINK** is an undirected version of **SINK**.

Note that **STCONN** is the strongest set of tautologies. We also show

Thm: STCONN has polynomial size Frege proofs.

The same proof will show:

Thm: STCONN has polynomial size TC^0-Frege proofs.

where TC^0-Frege means Frege plus counting gates, restricted to constant depth.

These upper bounds on proof size thus apply to all the tautologies.

Furthermore,

Thm: The **STCONN** principles of bounded width d have polynomial size resolution refutations.

Lower Bounds: Since **PHP** requires exponential size constant depth Frege proofs [K-P-W,P-B-I], so does every other tautology listed.

Formulation of STCONN

Recall **STCONN** is a combinatorial principle on a $d \times n$ grid graph. Vertex in i-th row and j-column is denoted (i, j). We express the negation of **STCONN** as a set of clauses. The variables in the **STCONN** tautology are $g_{\{\alpha,\beta\}}$ and $r_{\{\alpha,\beta\}}$, where α, β are adjacent grid vertices, and indicate the presence of a green (resp., red) edge between α and β. There are clauses that state

1. The subgraph of green edges has one edge incident on $(1, 1)$, one edge incident on (d, n), and every vertex has green degree either zero or two.
2. The corresponding clauses about the subgraph of red edges.
3. No vertex belongs to both a red and green edge.

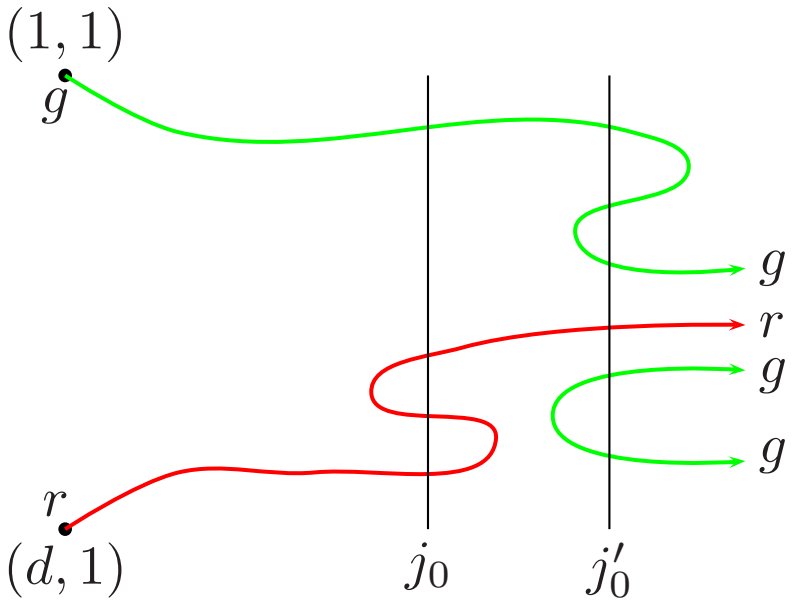
This makes $O(d \cdot n)$ clauses, each of size ≤ 4.

Converting the clauses expressing the negation of **STCONN** into a Boolean formula, **STCONN** is expressed as Σ_2 formula of size $O(d \cdot n)$.

Proof of STCONN in polynomial-size Frege

We give an intuitive proof, then argue that it can formalized with polynomial size Frege proofs.

The proof is a proof by contradiction. Assume we have a graph which satisfies the **STCONN** clauses; of course, it is a union of a green graph and a red graph. We take vertical crosssections of the graph, and obtain a "crossing sequence" which is a word over the alphabet $\{g, r\}$ that records the sequence of green and red edges that pass over the crosssectional split.



The crossing sequences for the two vertical lines above are "$grrr$" and "$gggrgg$".

The crossing sequences words are viewed as words in a group G.

The group G is generated by two generators "g" and "r". It is finitely presented by

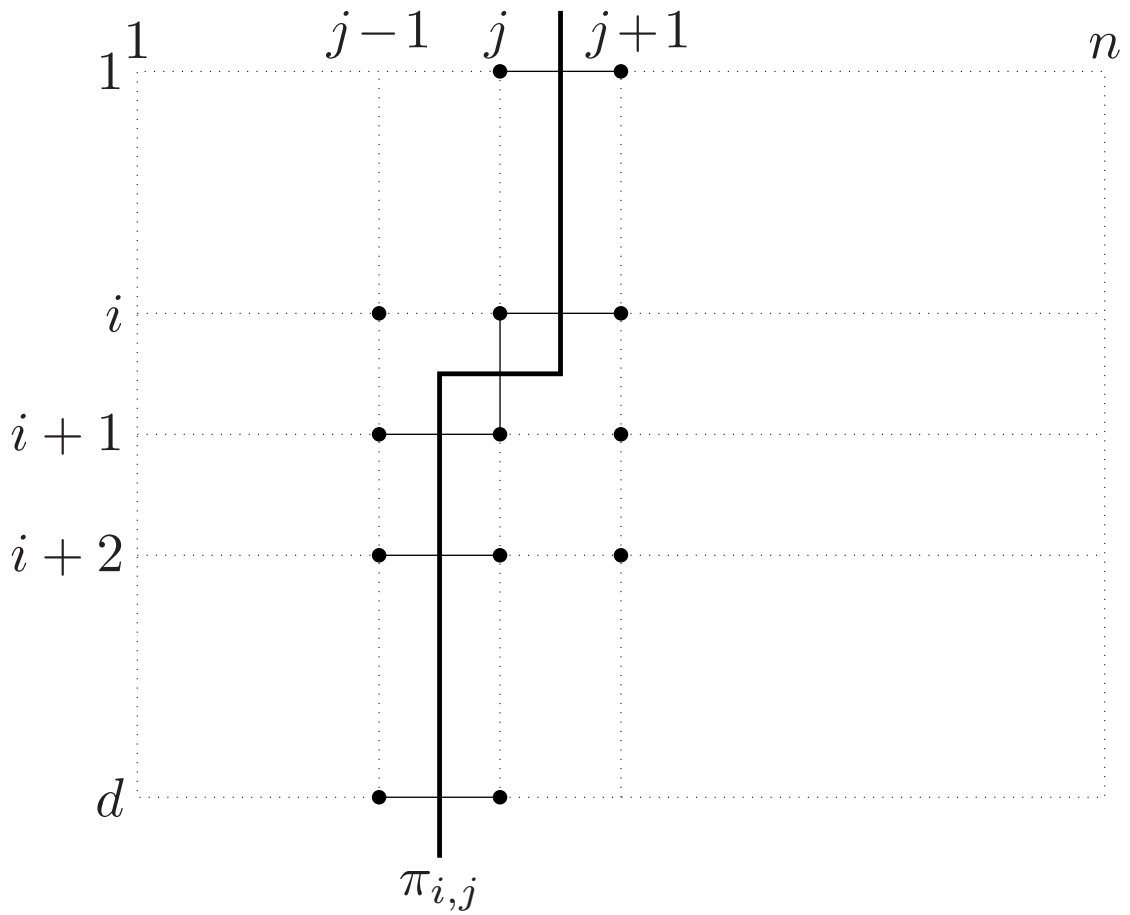
$$G \;=\; \langle g, r;\; g^2 = \epsilon, r^2 = \epsilon \rangle.$$

where ϵ is the empty word (the identity).

The intuitive idea of the proof of the **STCONN** is that the crossing sequences of any two adjacent columns in the grid graph represent the same element of G. But then, the first column has crossing sequence equal to "gr" in G and the last column has crossing sequence equal to "rg" in G. But, $rg \neq gr$ in G, which is a contradiction (which establishes the **STCONN** principle.

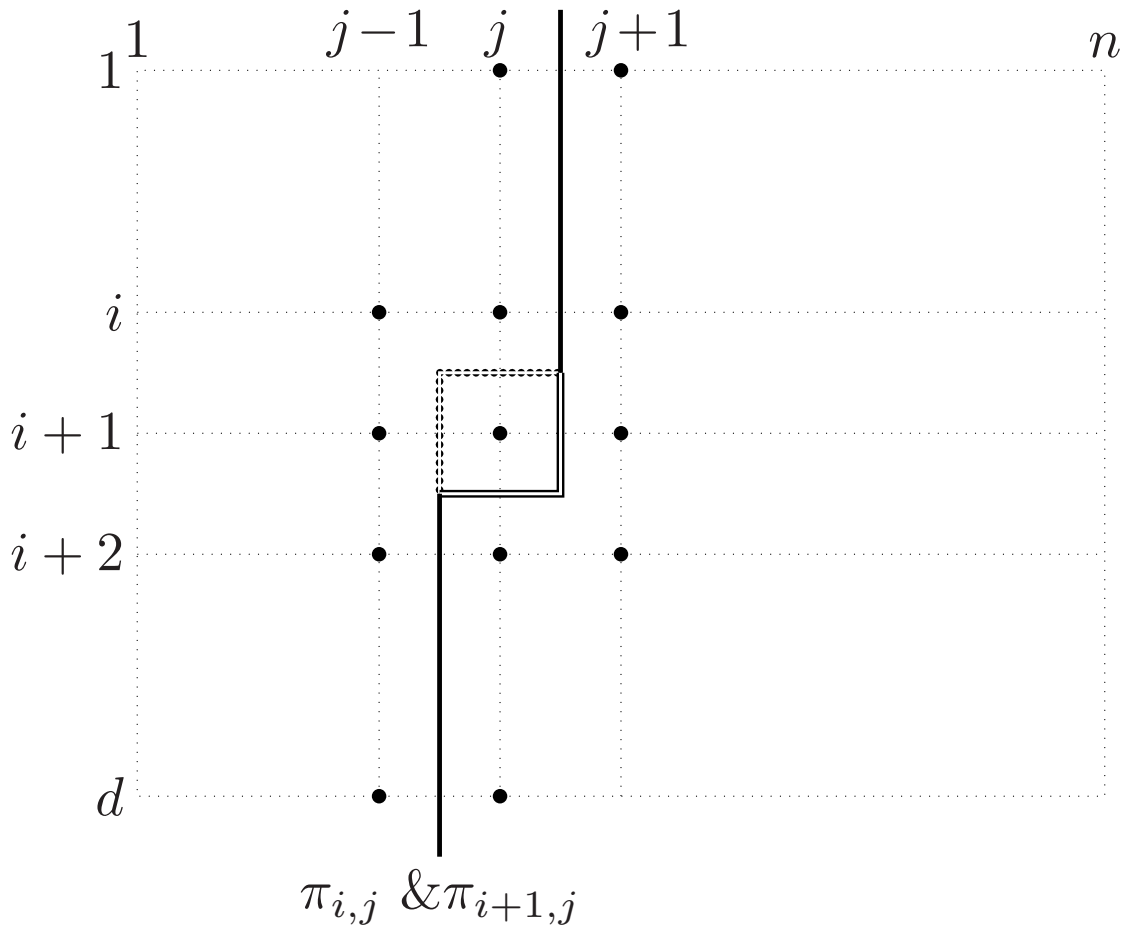
It remains to see how to formalize the intuitive proof in a Frege proof.

The first simplification is to consider more general vertical paths for crossing sequences (so it is not necessary to consider a whole column at once). For this, we choose crossing sequences for paths that are vertical except for single leftward jog.



The "vertical" $\pi_{i,j}$ crosses d potential horizontal edges in the graph and at most one potential vertical edge in the graph.

Each path $\pi_{i,j}$ differs from its successor $\pi_{i,j+1}$ in only two of the edges it crosses.



The crossing sequence is defined over the alphabet $\{g, r, e\}$, where e means "no edge". Two adjacent crossing sequences can differ in that a substring is "ge" replaced by "eg", or "gg" is replaced by "ee", or vice versa, or the same with r's in the roles of g's.

Thus, it is easy to see that if one crossing sequence is equal, in G, to "gr", then so is the next. The catch however, is to formalize the property of being equal to "gr" with polynomial size formulas.

Indeed, more general word problems on groups, even the word problem on the free group with two generators, are not known to be definable with polynomial size formulas.

Let $w = \alpha_1\alpha_2\cdots\alpha_n$, where each $\alpha_i \in \{g, r\}$.
W.l.o.g. n is even.
Grouping pairs of symbols, write w in the form

$$w \;=\; \beta_1\cdots\beta_m, \qquad m = n/2.$$

with each $\beta_i = \alpha_{2i-1}\alpha_{2i}$. Note that

$$\begin{array}{ll} gr \equiv (gr)^1 & gg \equiv (gr)^0 \\ rg \equiv (gr)^{-1} & rr \equiv (gr)^0. \end{array}$$

Then, let $c_i \in \{-1, 0, 1\}$ be such that $\beta_i \equiv (gr)^{c_i}$.
Then $w \equiv gr$ iff $\sum_i c_i = 1$.

To simplify the above construction, let

$$d_i = \begin{cases} 1 & \text{if } i \text{ is odd and } \alpha_i = g \\ & \quad \text{or if } i \text{ is even and } \alpha_i = r. \\ -1 & \text{otherwise.} \end{cases}$$

Clearly $d_{2i-1} + d_{2i} = 2c_i$, so $w \equiv gr$ iff $\sum_i d_i = 2$.

Since summation is expressible with polynomial size formulas, and since Frege systems can prove basic facts about summation, polynomial size Frege systems are strong enough to simple local facts about words over the alphabet $\{g, r\}$.

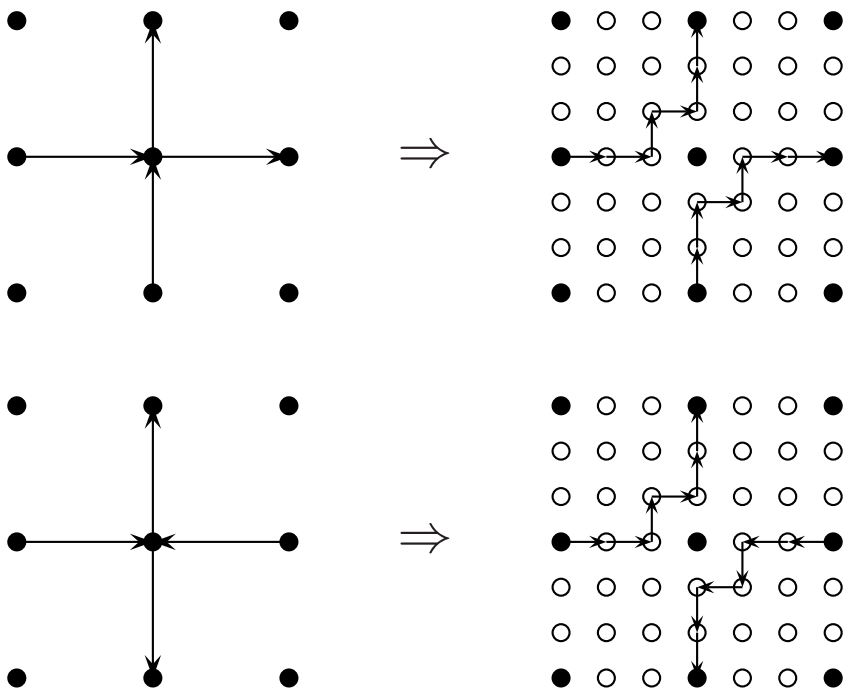
Counting can also be used to remove the e's from the crossing sequences.

The rest of the proof of **STCONN** with polynomial size Frege proofs is standard and straightforward. □

Theorem: 2SINK $\preccurlyeq_{cd\mathcal{F}}$ SINK.

2SINK is like **SINK**: formulated with directed grid graph. One vertex has out-degree one, in-degree zero. The rest have in-degree equal to out-degree. Unlike **SINK**, in- and out-degrees may equal 2.

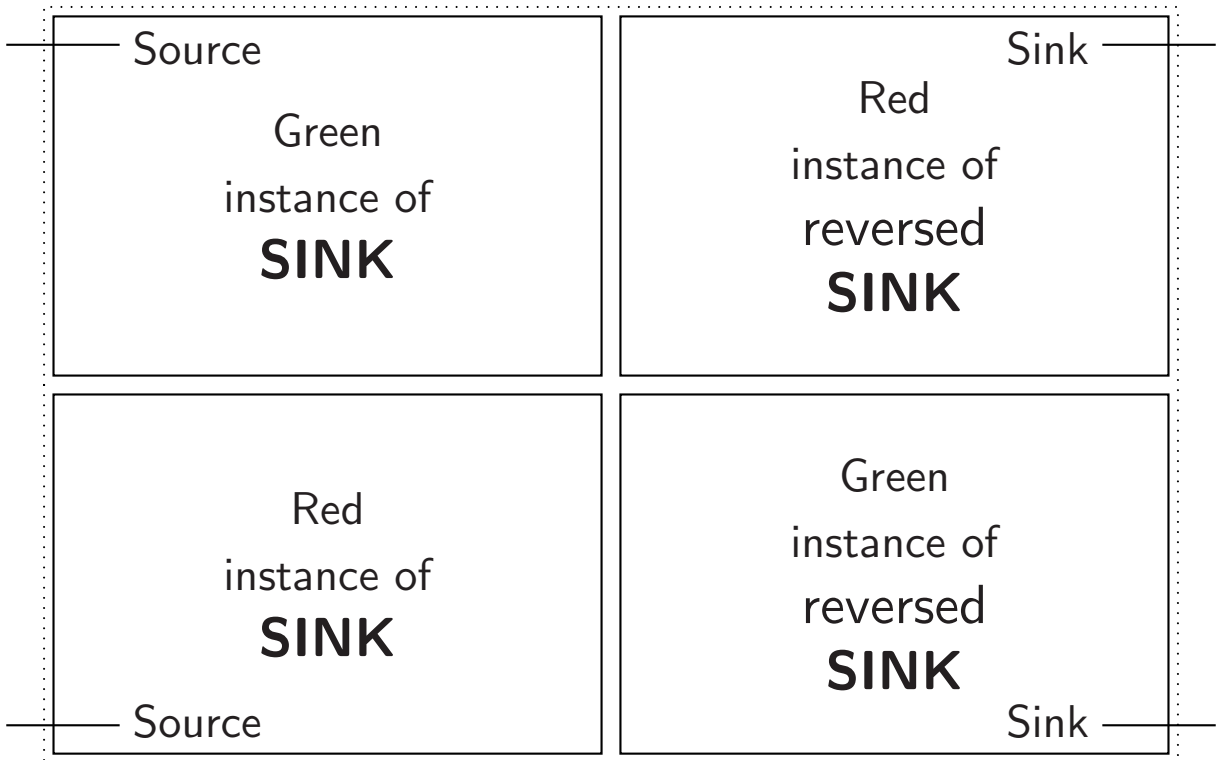
Proof of Theorem:



SINK $\preccurlyeq_{cd\mathcal{F}}$ DSTCONN $\preccurlyeq_{cd\mathcal{F}}$ STCONN

DSTCONN is the directed version of **STCONN**. To reduce **DSTCONN** to **STCONN** "erase the arrowheads" and change edges to undirected.

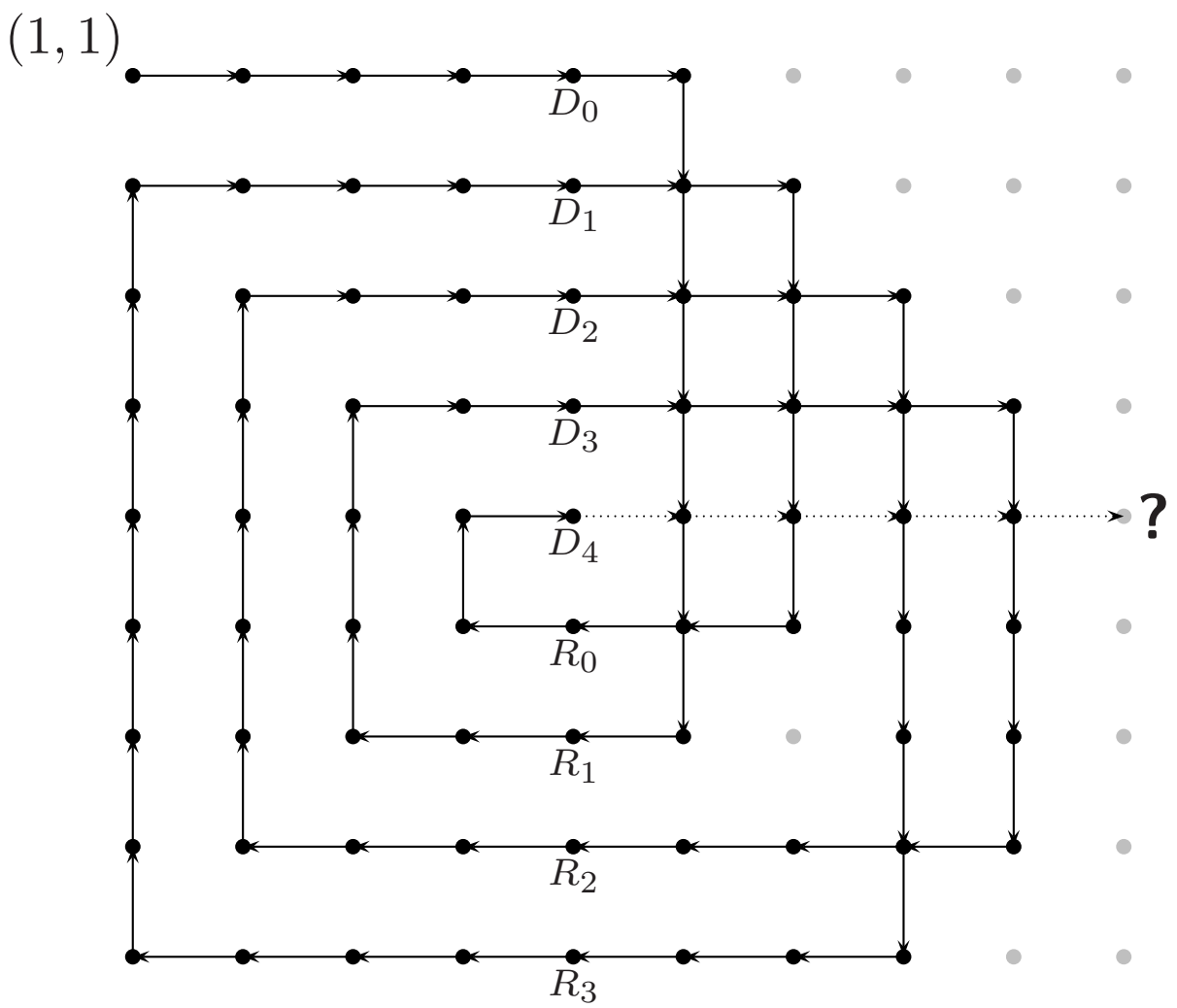
Proof of SINK $\preccurlyeq_{cd\mathcal{F}}$ DSTCONN:



The instances of SINK are located so that the source nodes are at the positions indicated.

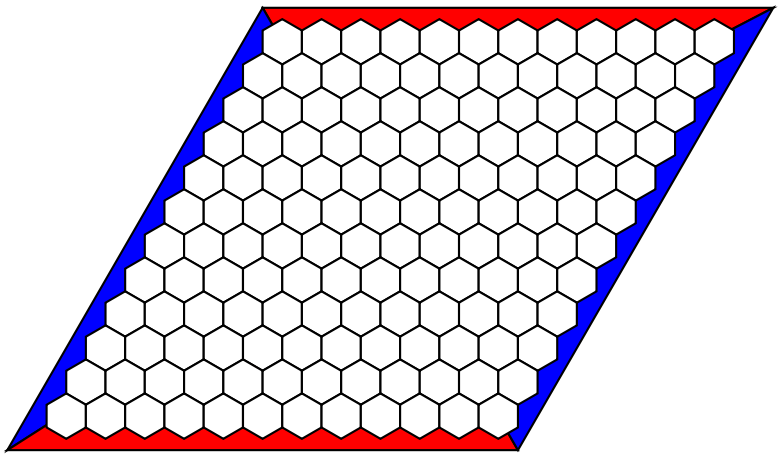
Theorem: PHP $\preccurlyeq_{cd\mathcal{F}}$ 2SINK

Proof: (**PHP** is the 1-1, onto pigeonhole principle.)



On the left half, pair R_i with D_{n-i}. On right half, pair D_i with $R_{f(i)}$, where $f : [n+1] \to [n]$ violates the pigeonhole principle.

The Game of HEX



Two players alternate coloring the hexagons. One player colors hexagons red, the other blue. The winner is the first to establish a path of his color that joins the same colored opposite sides of the board.

Combinatorial facts:

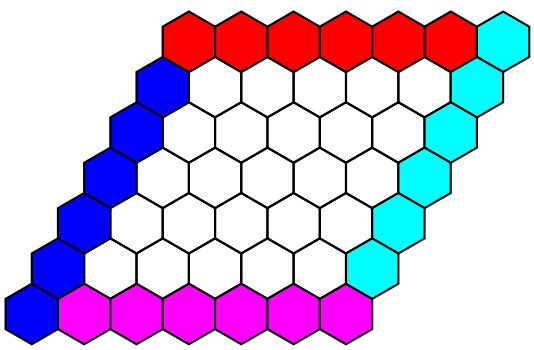
- There can be only one winner (there cannot be both a red path and a blue path joining the opposite red (resp., blue) sides of the board.
- Every play of the game has a winner.
  (This is the HEX tautology.)
- The first player has a winning strategy.

The HEX Tautology - Formalized

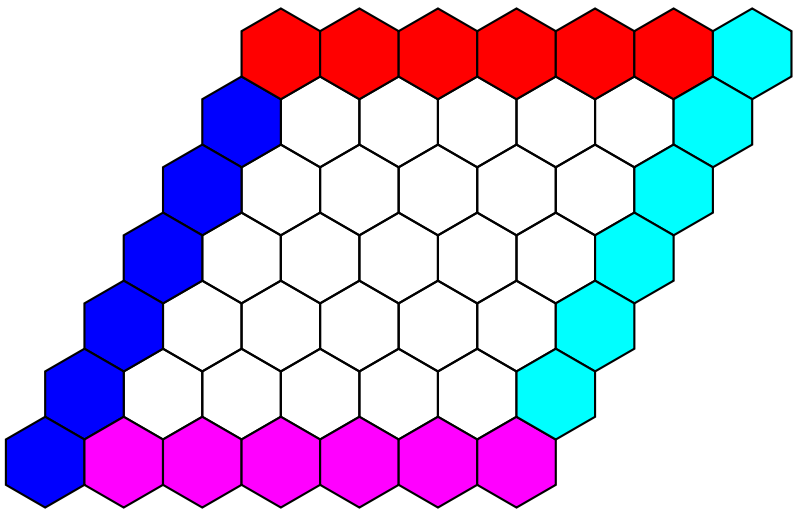
The **HEX** tautology expresses the fact that once the board is completely filled in, one of the players must have won the game. For each game board hexagon h, there are variables R_h, B_h, M_h, and C_h ("red", "blue", "magenta", "cyan"). The intuitive idea is that red hexagon connect to the upper border, blue to the left border, magenta to the bottom, cyan to the right. (Based on a construction of Urquhart.)

Thm: The following is inconsistent:

- Each hexagon has one color (or: a color).
- Every border hexagon has the right color.
- No red and magenta hexagons are adjacent.
- No blue and cyan hexagons are adjacent.



Thm: HEX $\preccurlyeq_{cd\mathcal{F}}$ SINK.

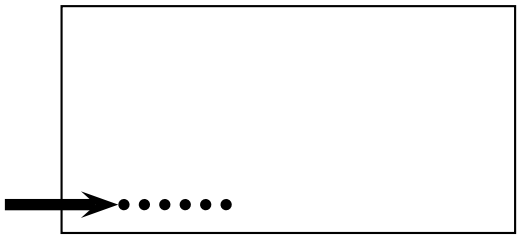


The proof of Gale about Hex games always having a winner can be adapted to prove the theorem.

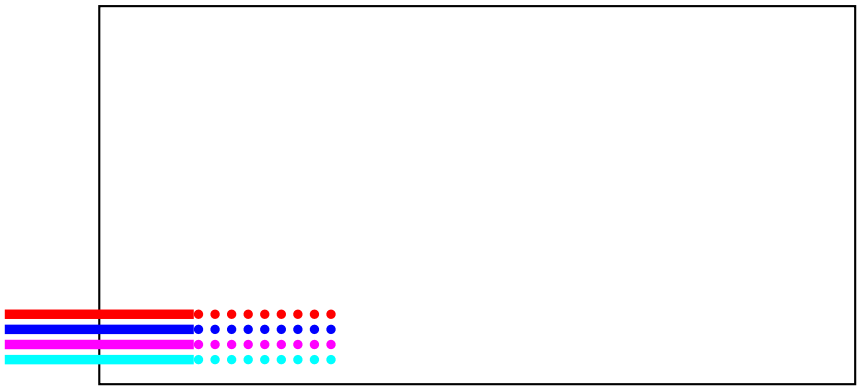
The proof is by contradiction. Suppose there is a violation of the **HEX** tautology. Wherever, a red and a blue hexagon are adjacent, place a directed edge with red on its left side. These edges create a violation of the **SINK** principle. □

Thm: SINK $\preccurlyeq_{cd\mathcal{F}}$ HEX.

Suppose there is a contradiction to **SINK**:



Turn the path in the **SINK** graph into four parallel paths colored, from left to right, Red, Blue, Magenta, Cyan; then remove the directedness. The resulting graph is topologically equivalent to a violation of the **HEX** tautology:



Some Open Problems

1. Is the word problem for the free group with two generators in Alogtime? Does it have polynomial size formulas?

2. Separate depth d Frege systems and depth $d+1$ Frege systems using formulas of depth $< d$.

3. Solve the analogous problem about the conservativity of $T_2^{d+1}(\alpha)$ over $T_2^d(\alpha)$.

4. Investigate connections between the fact that various tautologies have short Frege proofs, and the decision classes of Papadimitriou ['90,'94] and Beame-Cook-Edmonds-Impagliazzo-Pitassi ['98]. Gale ['79] also discusses connections between these problems and Brower fixed point theorem (equivalent to every Hex game having a winner.) Also, Gale shows Jordan curve theorem is equivalent to every Hex game having a single winner.