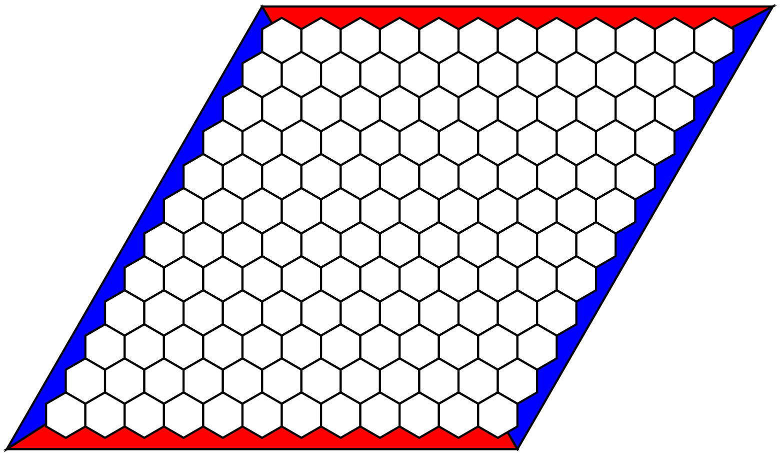
# Propositional Proofs of Hex Tautologies and st-Connectivity

Sam Buss
Department of Mathematics
U.C. San Diego

SLALM'12 - San Jose, Costa Rica
January 2004

# 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.

# 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.

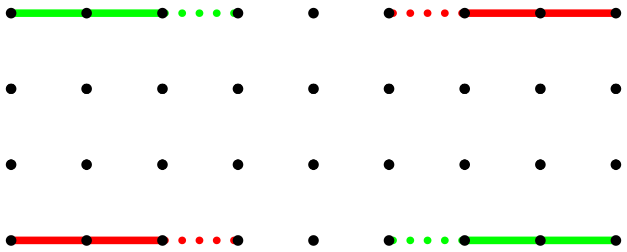
**Thm:** There is a directed path from $s$ to $t$.

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.

$\Pi_d$ and $\Sigma_d$ 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 $\Pi_d$-complete.

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

Unfortunately, this turns out to be false.

# 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 $\vee$. 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, $\Gamma$ a set of formulas and $A$ a formula. Then a $P$-proof of $A$ from $\Gamma$ is defined as usual. A $P$-refutation of $\Gamma$ is a $P$-proof of a contradiction from $\Gamma$.

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

**Open problem:** Are there sets of clauses ($\Pi_2$-formulas) which have polynomial size, depth $d+1$ Frege refutations, but require superpolynomial size, depth $d$ Frege refutations?

# Connections with Bounded Arithmetic
# The Paris-Wilkie Translation

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

**Def'n:** Let $A(x)$ be a $\Sigma^b_d$-formula. Then, $[\![A]\!]$ is a family of polynomial-size $\Sigma$-depth $d$ formulas, expressing the condition $\forall x A(x)$. Free variables in the formulas represent the bits of the integer $x$. Quantifiers are changed into unbounded $\vee$'s and $\wedge$'s.

**Def'n:** [Buss] $S^i_2$ and $T^i_2$ are theories of arithmetic, with length induction (resp., induction) on $\Sigma^b_i$-formulas.

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

**Uniform version of open problem:** For $i \leq j < k$, is $T^k_2(\alpha)$ conservative over $T^j_2(\alpha)$ with respect to $\Sigma^b_i(\alpha)$-formulas?

# 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:** [Buss]

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

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 $\alpha$, $\beta$ are adjacent grid vertices, and indicate the presence of a green (resp., red) edge between $\alpha$ and $\beta$. 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.

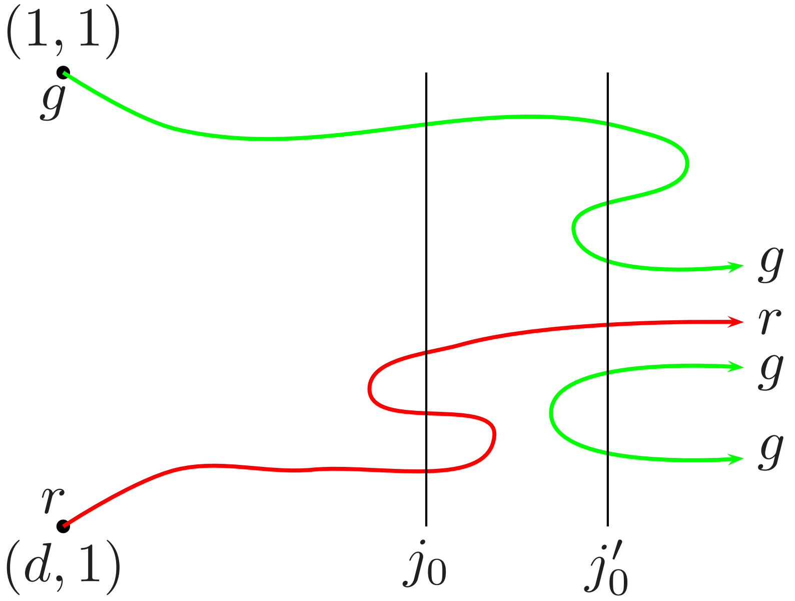
This makes $O(d \cdot n)$ clauses, each of size $\leq 4$.

Converting the clauses expressing the negation of **STCONN** into a Boolean formula, **STCONN** is expressed as $\Sigma_2$ 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

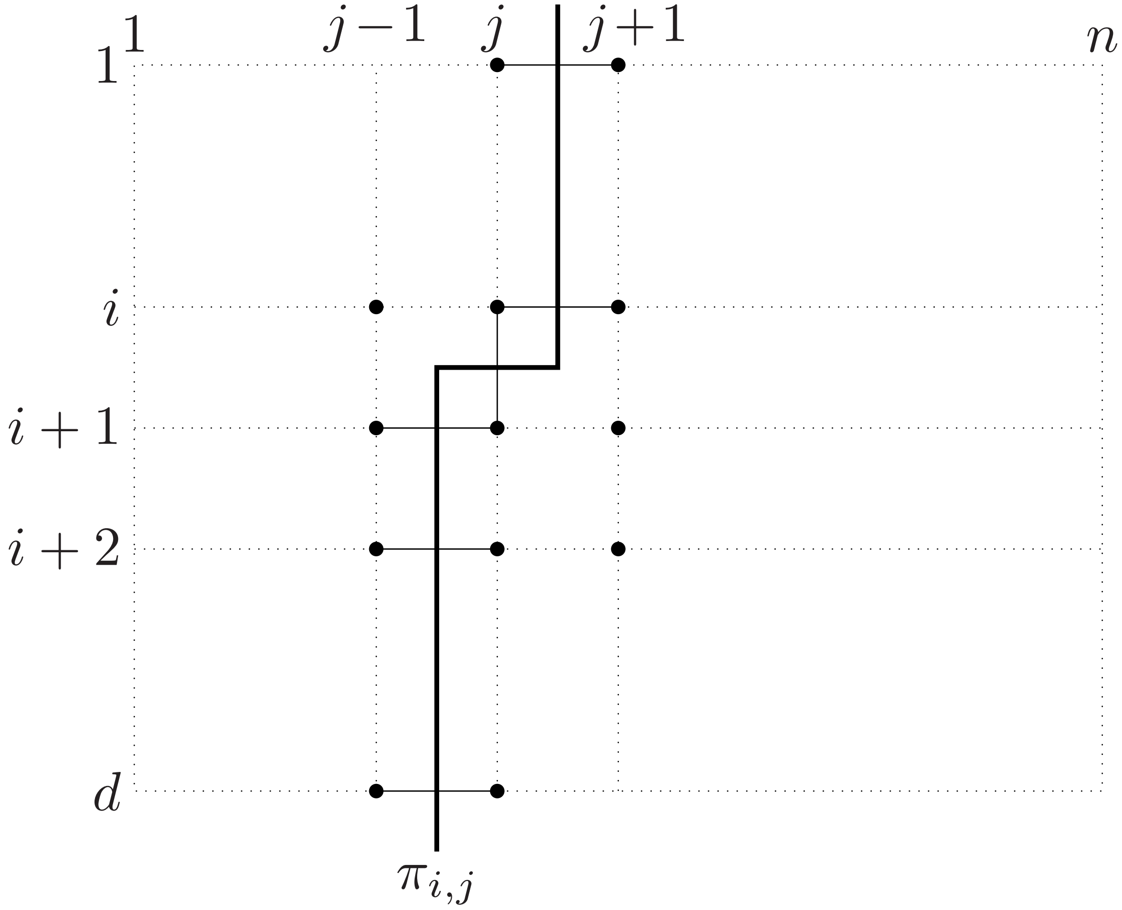
$$G \;=\; \langle g, r;\; g^2 = \epsilon, r^2 = \epsilon \rangle.$$

where $\epsilon$ 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.

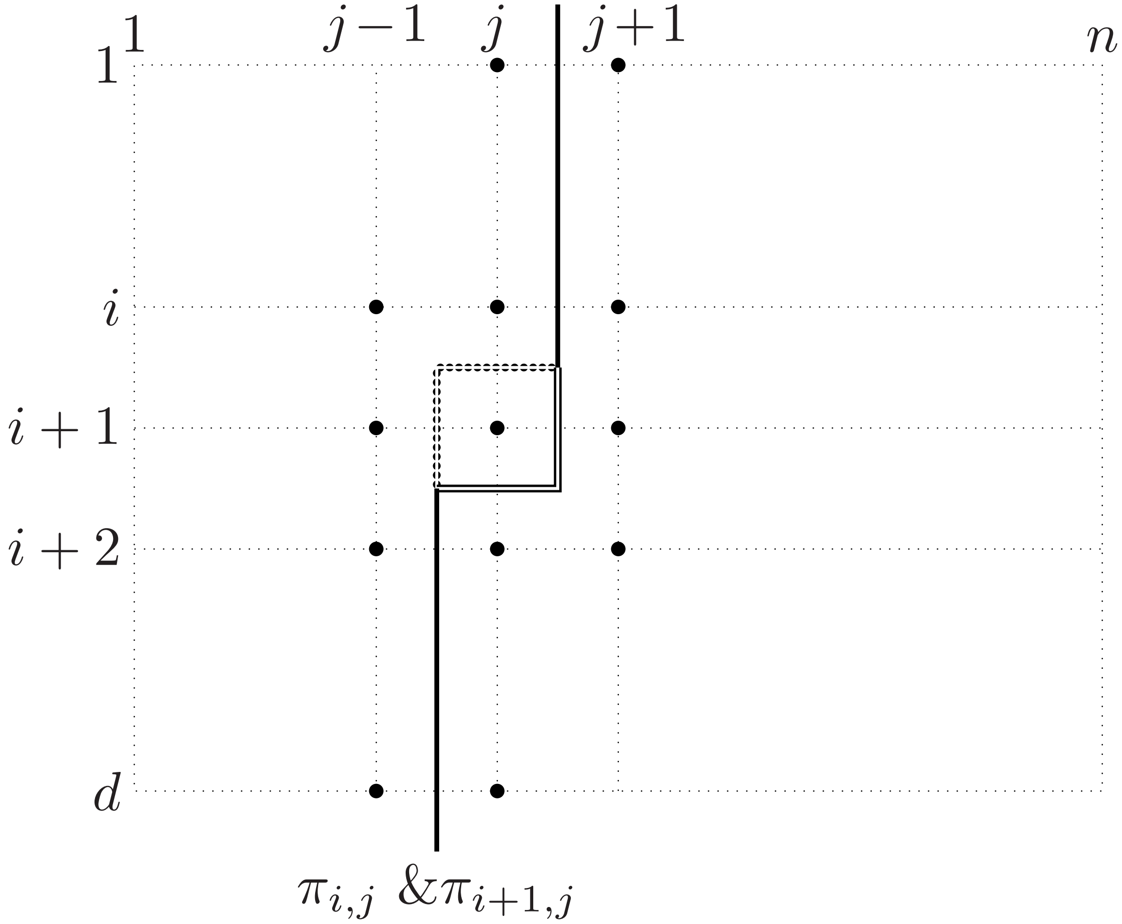
It remains to see how to formalize the intuitive proof in a Frege proof.

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

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

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 $\{g, r\}$.

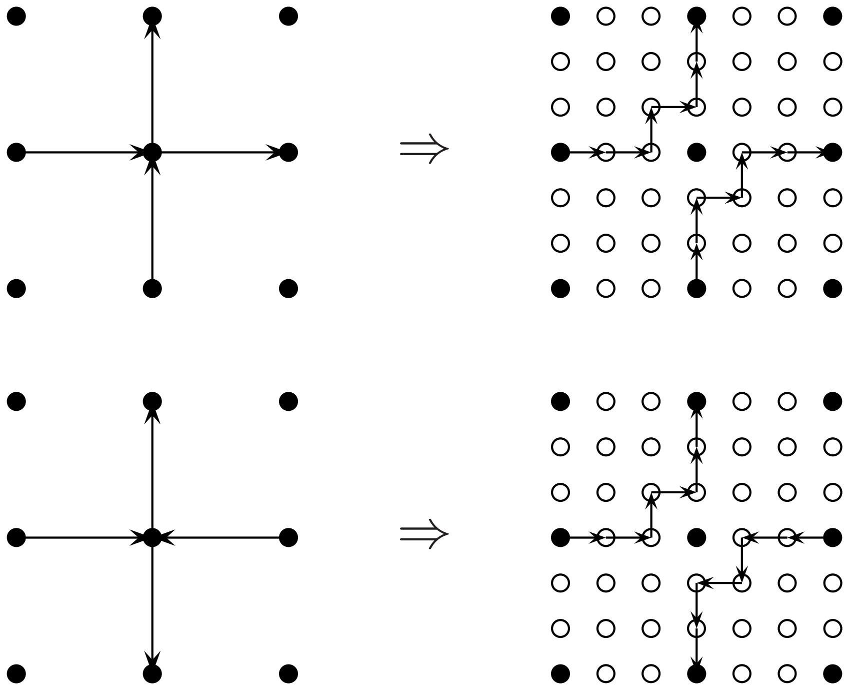
Counting can also be used to remove the $e$'s from the crossing sequences.

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.

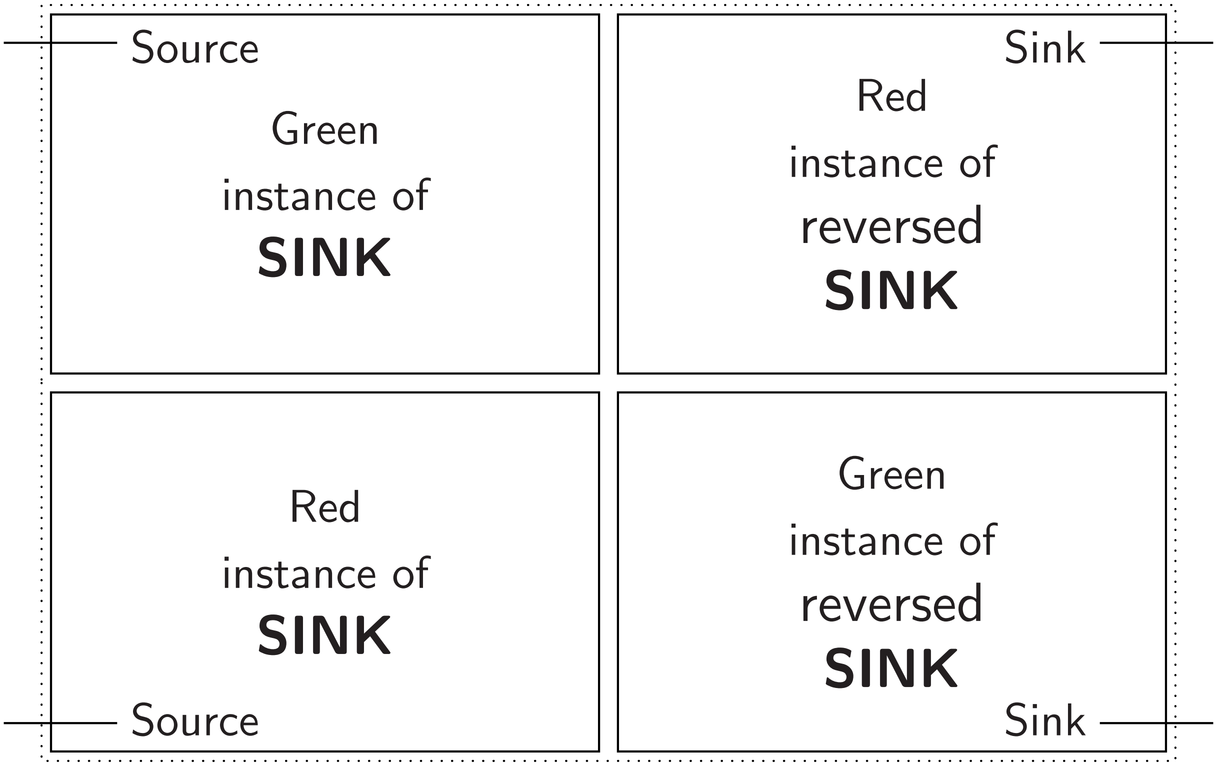
**Proof of Theorem:**



# 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.

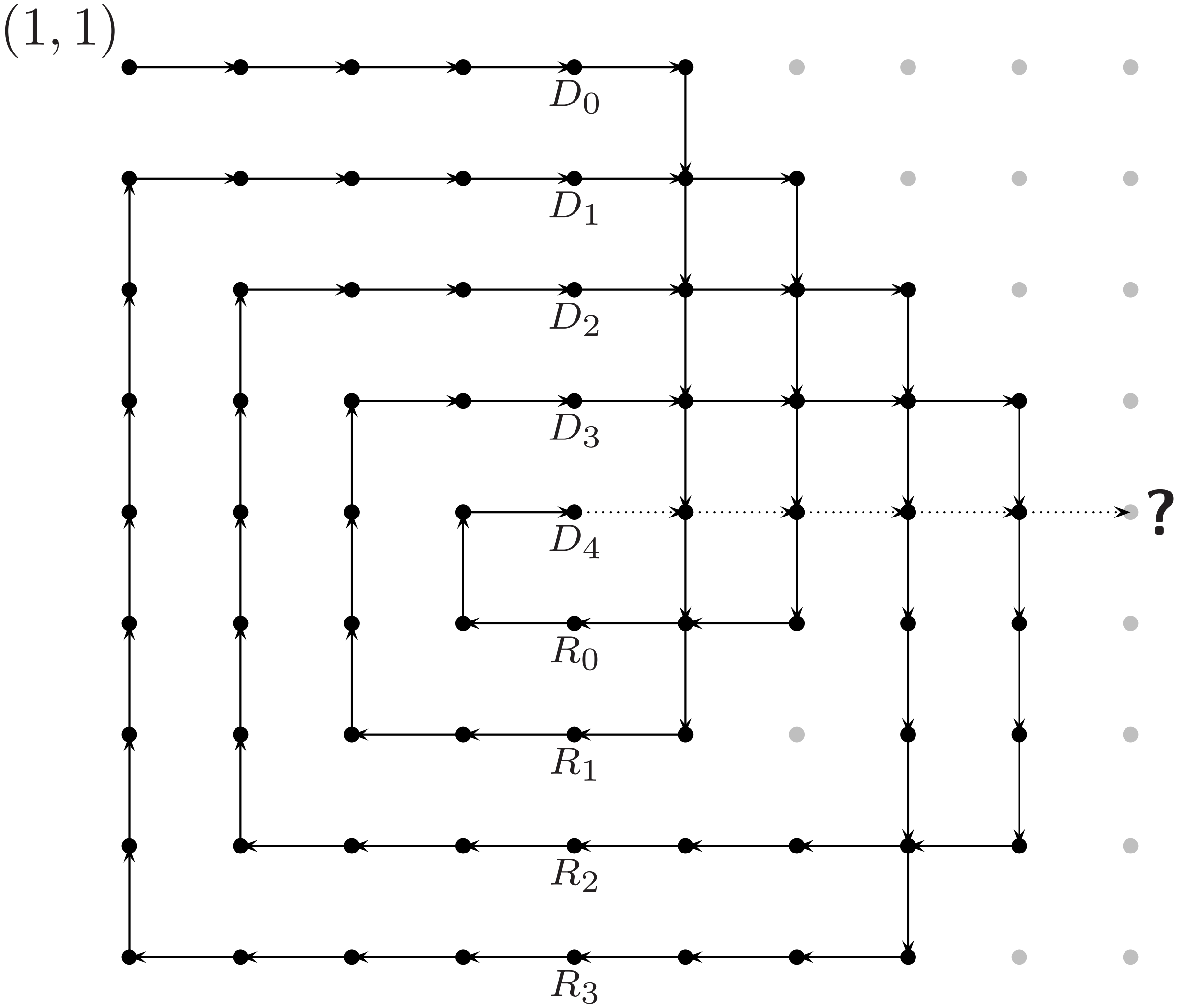
**Proof of SINK $\preccurlyeq_{cd\mathcal{F}}$ DSTCONN:**


Source
Green instance of **SINK**
Sink
Red instance of reversed **SINK**
Red instance of **SINK**
Source
Green instance of reversed **SINK**
Sink

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.)



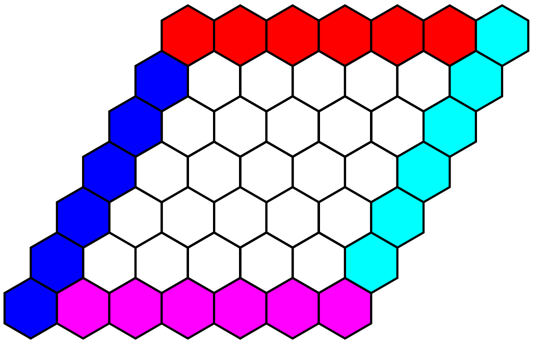
On the left half, pair $R_i$ with $D_{n-i}$. On right half, pair $D_i$ with $R_{f(i)}$, where $f : [n+1] \to [n]$ violates the pigeonhole principle.

# The HEX Tautology - Formalized

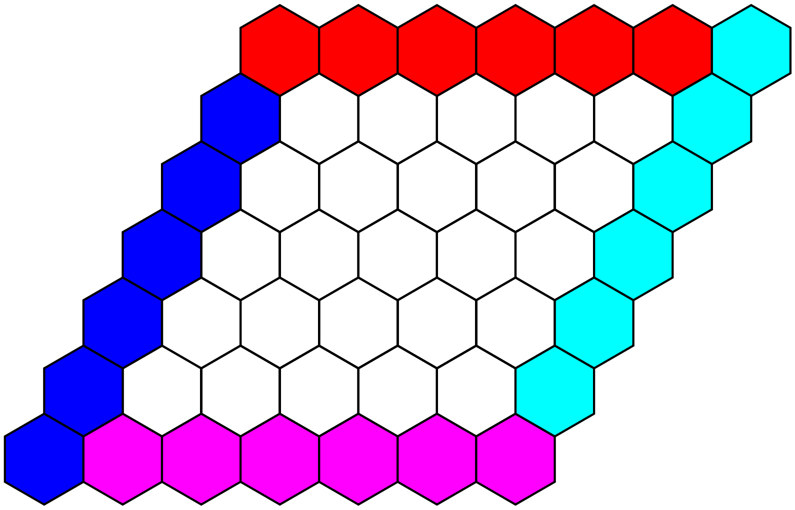
The **HEX** tautology expresses the fact that once the board is completely filled in, one of the players must have won the game. For each game board hexagon $h$, there are variables $R_h$, $B_h$, $M_h$, and $C_h$ ("red", "blue", "magenta", "cyan"). The intuitive idea is that red hexagon connect to the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

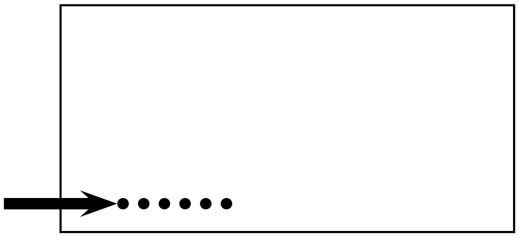


The proof of Gale about Hex games always having a winner can be adapted to prove the theorem.

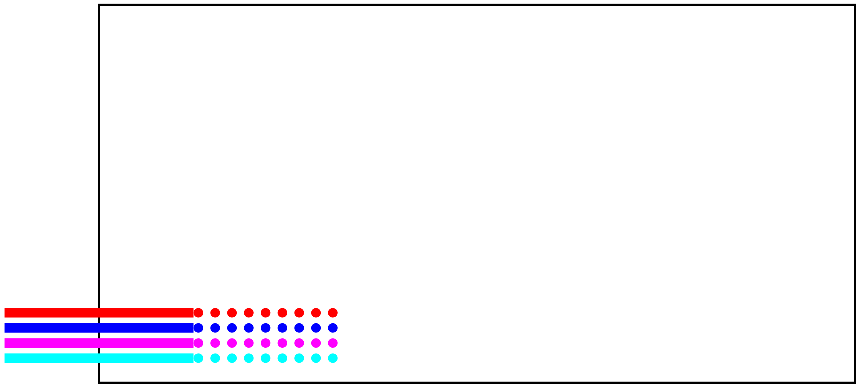
The proof is by contradiction. Suppose there is a violation of the **HEX** tautology. Wherever, a red and a blue hexagon are adjacent, place a directed edge with red on its left side. These edges create a violation of the **SINK** principle. □

**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.