Approaching the minimum clues Sudoku problem via the polynomial method

John Schmitt

Joint work with Aden Forrow

Outline of this talk

1. Sudoku and Shidoku and the minimum number of clues problem
   1. Brief facts
   2. Redundancy in the rule set
2. Tools from the polynomial method
   1. Alon's Combinatorial Nullstellensatz
   2. Schauz's Coefficient Formula
   3. Two quick corollaries to this formula
3. Apply the polynomial method to solve the minimum number of clues Shidoku problem

Basic Facts

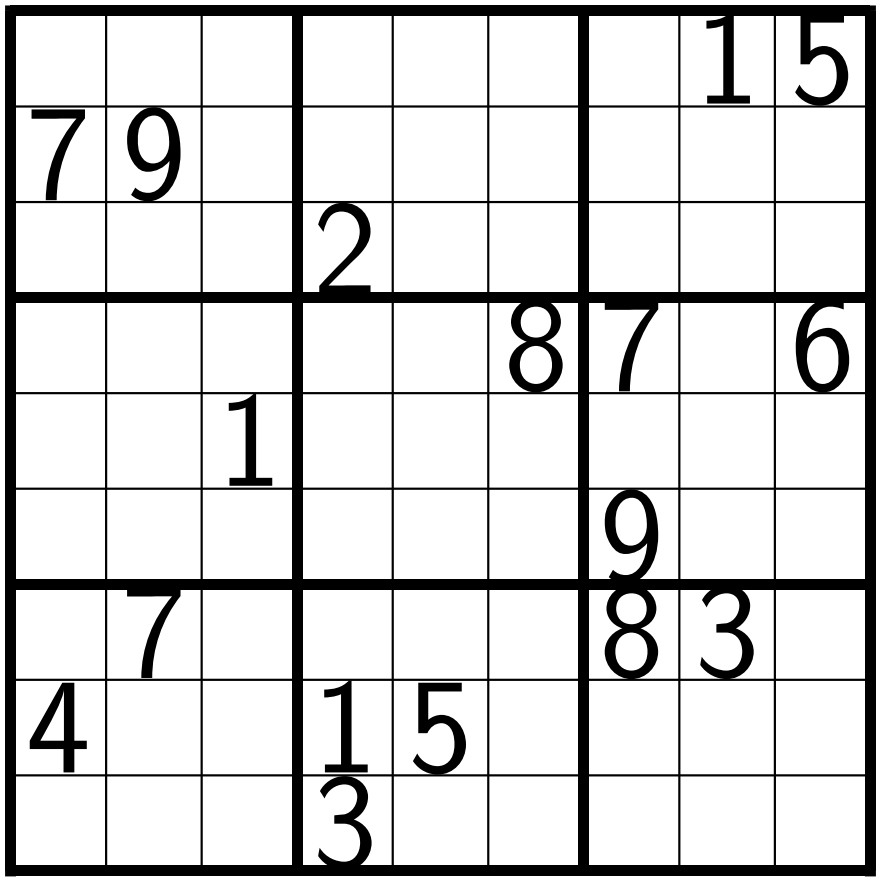


Figure : A 17-clue Sudoku puzzle

Basic Facts

- Felgenhauer and Jarvis computed that there are 6,670,903,752,021,072,936,960 completed Sudoku squares (i.e. about 6.671×10^{21}),
- and taking into account symmetries and relabeling, there are 5,427,730,538 (i.e. about 5.428×10^{9}).

Conjecture

The fewest number of clues in a Sudoku puzzle with a unique completion is 17.

Conjecture

The fewest number of clues in a Sudoku puzzle with a unique completion is 17.

Gordon Royle has a collection of 49,151 inequivalent Sudoku puzzles with 17 clues, see http://school.maths.uwa.edu.au/∼gordon/sudokumin.php.

Conjecture

The fewest number of clues in a Sudoku puzzle with a unique completion is 17.

Gordon Royle has a collection of 49,151 inequivalent Sudoku puzzles with 17 clues, see http://school.maths.uwa.edu.au/∼gordon/sudokumin.php.

On January 1, 2012, G. McGuire, B. Tugemann, G. Civario announced that they proved the conjecture.

Using case reductions and clever search strategies, they reduced the exhaustive computer search to...

Conjecture

The fewest number of clues in a Sudoku puzzle with a unique completion is 17.

Gordon Royle has a collection of 49,151 inequivalent Sudoku puzzles with 17 clues, see http://school.maths.uwa.edu.au/∼gordon/sudokumin.php.

On January 1, 2012, G. McGuire, B. Tugemann, G. Civario announced that they proved the conjecture.

Using case reductions and clever search strategies, they reduced the exhaustive computer search to...a year-long computation, with 7.1 million core hours on an SGI Altic ICE 8200EX cluster with 320 nodes, each of which consisted of two Intel Xeon E5650 hexcore processors with 24GB of RAM.

Description of method of McGuire et al.:

1. Make a catalogue of all 5,427,730,538 Sudoku squares.
2. Search within a square for puzzles with 16 clues whose solution is the given square.
3. Run through the catalogue of all completed squares and apply program to each square in turn.

	1	2	
1			3

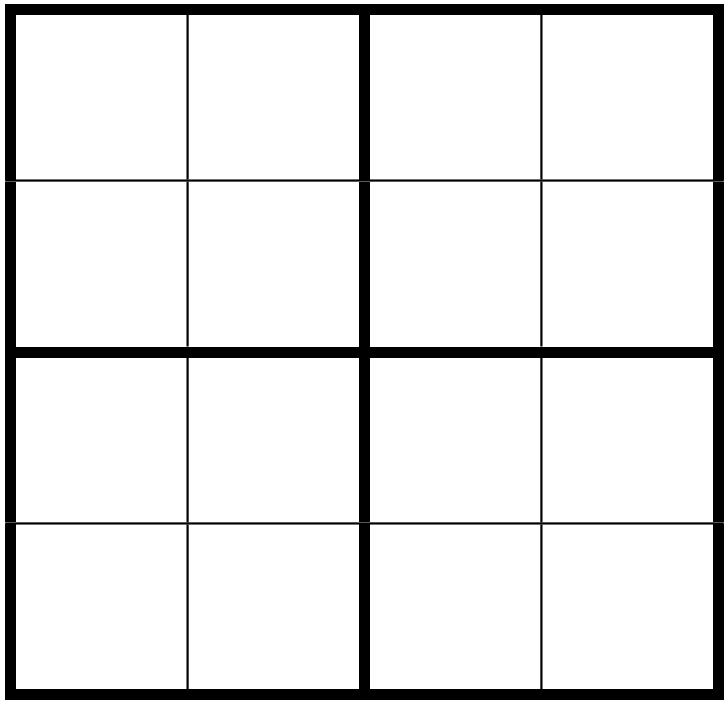
Figure : A 4-clue Shidoku puzzle

There are 288 completed Shidoku squares.

Theorem

The fewest number of clues in a Shidoku puzzle with a unique completion is 4.

The Shidoku board and its rule set lead naturally to a graph SUD_2, which has 16 vertices and 56 edges.



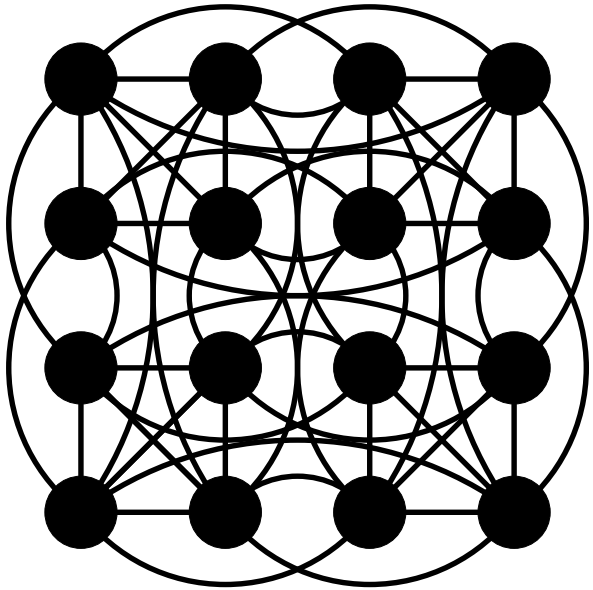


Figure : The 16-vertex 56-edge Shidoku graph

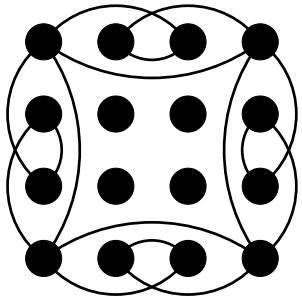


Figure : G_1 is a subgraph of SUD_2 containing a maximal set of *redundant* edges

Focus on top chute, i.e. top two rows (or top two boxes).

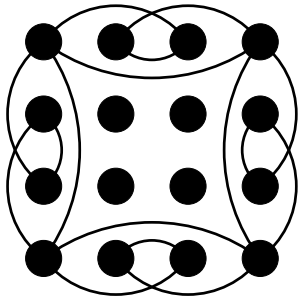


Figure : G_1 is a subgraph of SUD_2 containing a maximal set of *redundant* edges

Focus on top chute, i.e. top two rows (or top two boxes). Fill top chute with 8 numbers, with values from $\{1, 2, 3, 4\}$. Box constraints say there is exactly one of each in each box, which means two of each in the chute. Since second row is present, exactly one of each of these is in row 2. This leaves exactly one of each in row 1.

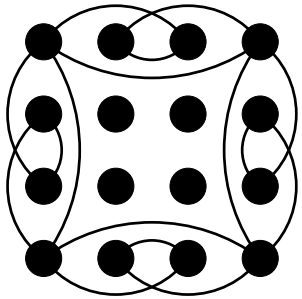


Figure : G_1 is a subgraph of SUD_2 containing a maximal set of *redundant* edges

Focus on top chute, i.e. top two rows (or top two boxes). Fill top chute with 8 numbers, with values from $\{1, 2, 3, 4\}$. Box constraints say there is exactly one of each in each box, which means two of each in the chute. Since second row is present, exactly one of each of these is in row 2. This leaves exactly one of each in row 1. Repeat this argument three times: bottom chute, left chute and right chute.

The eight redundancy graphs with 16 edges

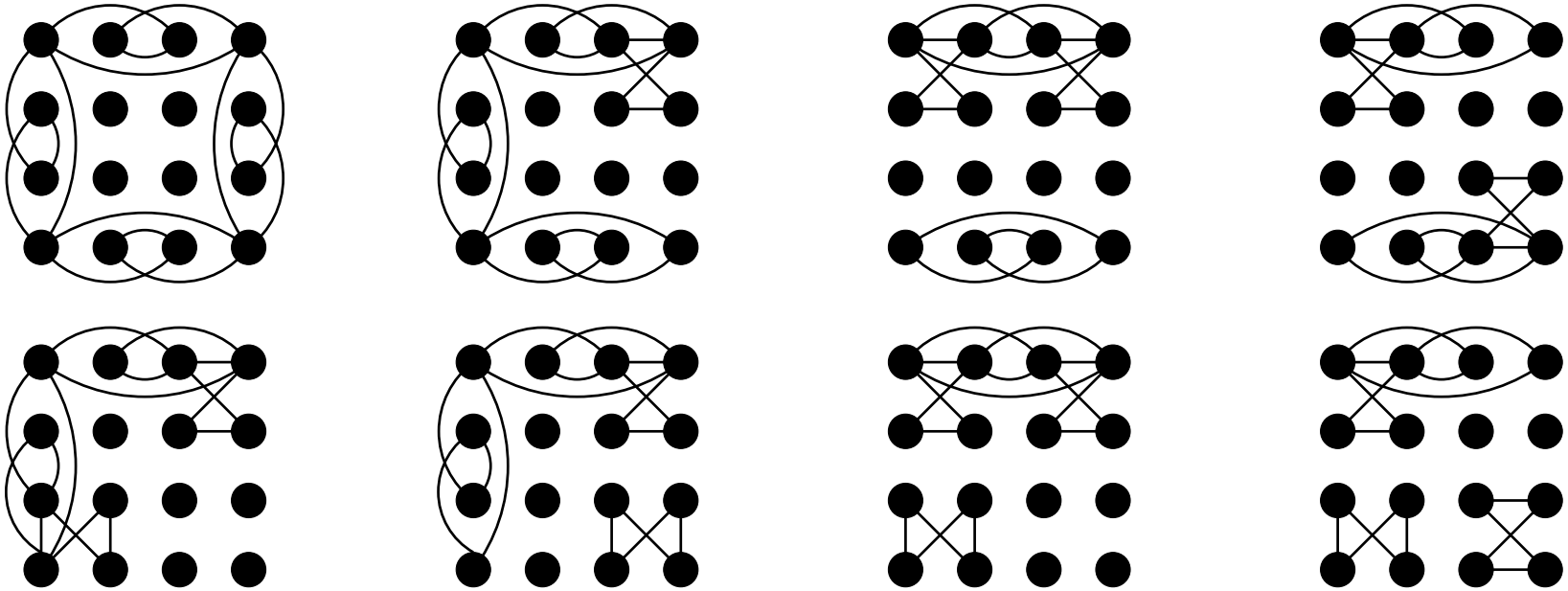
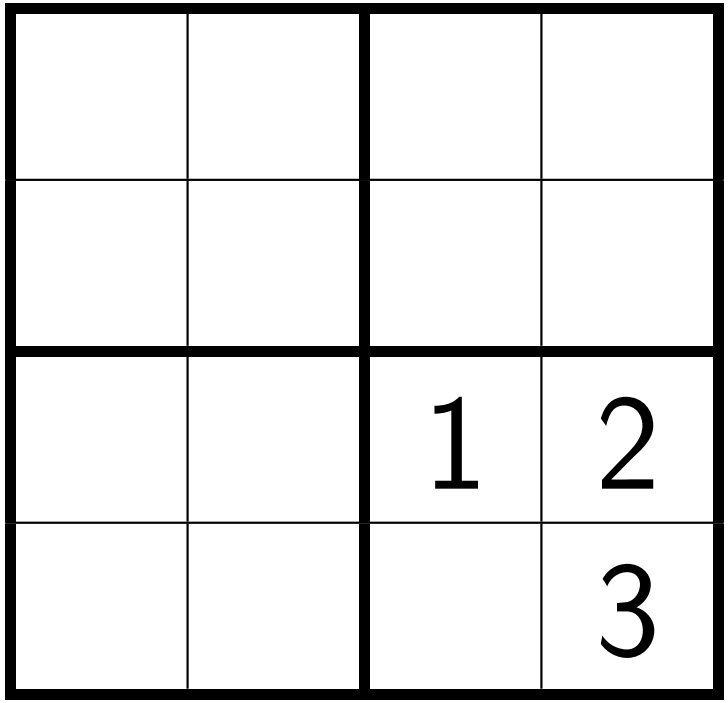


Figure : $G_1, \ldots G_8$, from left to right, top to bottom

B. Demoen and M.G. de la Banda (2012, 2013)


1 2
3

x_1	x_2	x_3	x_4
x_5	x_6	x_7	x_8
x_9	x_{10}	1	2
x_{11}	x_{12}	x_{13}	3

Assign variables to unfilled cells.

x_1	x_2	x_3	x_4
x_5	x_6	x_7	x_8
x_9	x_{10}	1	2
x_{11}	x_{12}	x_{13}	3

Assign variables to unfilled cells. Pick one of $G_1, \ldots, G_8$; here, we'll pick G_7.

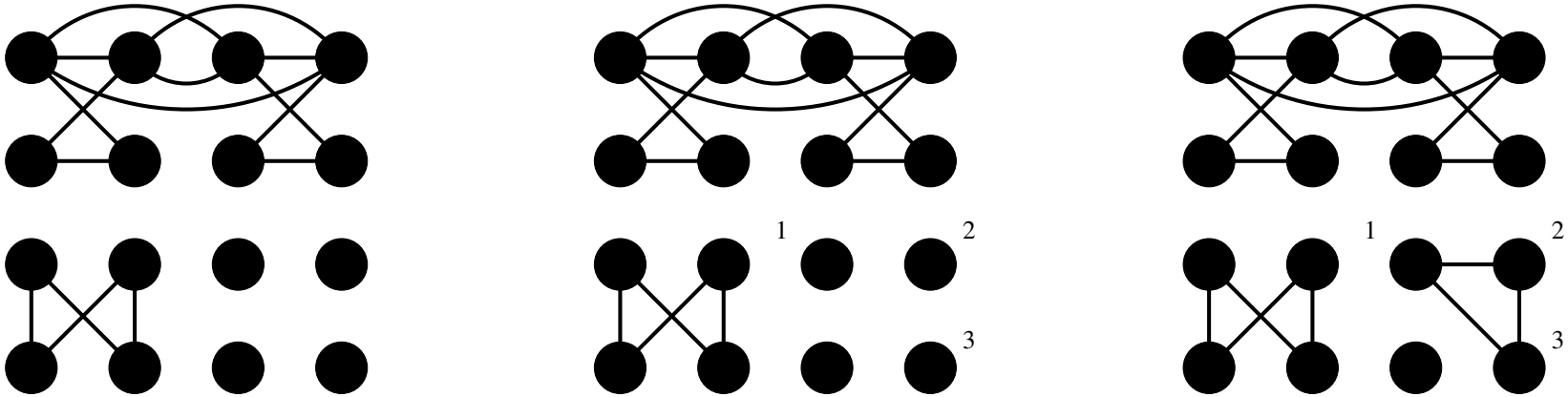


Figure : L-to-R: G_7; and with clues; and more edges deleted

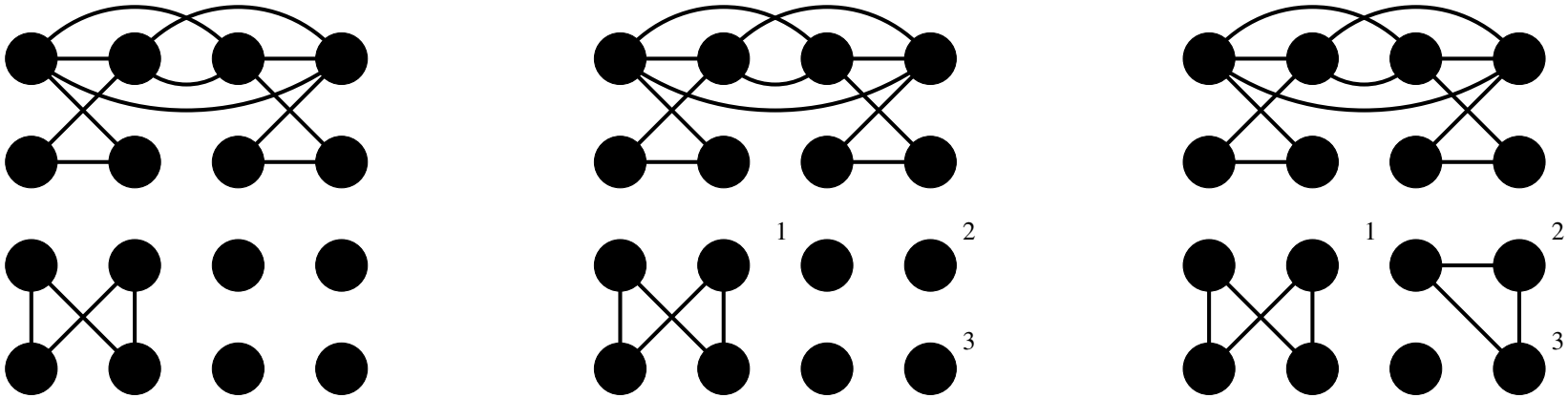


Figure : L-to-R: G_7; and with clues; and more edges deleted

Delete the 19 edges contained in right-most graph from SUD_2; obtain a graph G with 56-19=37 edges.

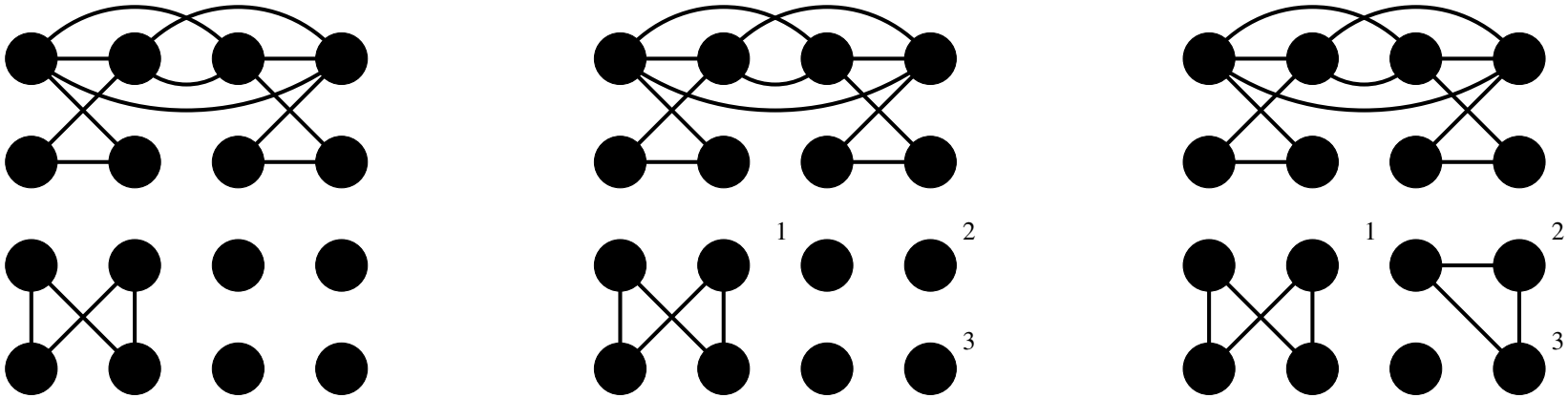


Figure : L-to-R: G_7; and with clues; and more edges deleted

Delete the 19 edges contained in right-most graph from SUD_2; obtain a graph G with 56-19=37 edges.
Write down the *graph polynomial* f_G of the resulting graph:

$$f_G = f_G(x_1, \ldots, x_{13}) \in \mathbb{R}[x_1, \ldots, x_{13}].$$

$f_G =$
$(x_1 - x_5)(x_1 - x_9)(x_1 - x_{11})(x_2 - x_6) \ldots (x_3 - 1) \ldots (x_4 - 2)(x_4 - 3) \ldots (x_{13} - 3)$

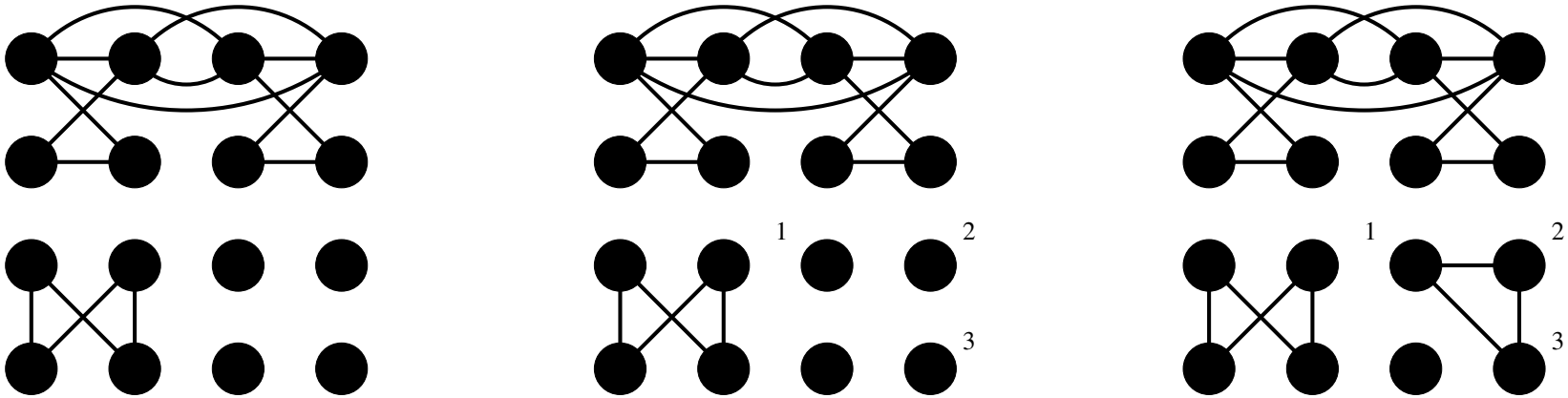


Figure : L-to-R: G_7; and with clues; and more edges deleted

Delete the 19 edges contained in right-most graph from SUD_2; obtain a graph G with 56-19=37 edges.
Write down the *graph polynomial* f_G of the resulting graph:

$$f_G = f_G(x_1, \ldots, x_{13}) \in \mathbb{R}[x_1, \ldots, x_{13}].$$

$f_G =$
$(x_1 - x_5)(x_1 - x_9)(x_1 - x_{11})(x_2 - x_6) \ldots (x_3 - 1) \ldots (x_4 - 2)(x_4 - 3) \ldots (x_{13} - 3)$
That is, f_G is the product of 37 linear factors, each of which is one of the following forms: $(x_a - x_b)$ or $(x_a - c_b)$, where c_a is the '**c**olor' of vertex a.

$f_G =$
$(x_1 - x_5)(x_1 - x_9)(x_1 - x_{11})(x_2 - x_6) \ldots (x_3 - 1) \ldots (x_4 - 2)(x_4 - 3) \ldots (x_{13} - 3)$
When is f_G equal to zero?

$f_G =$
$(x_1 - x_5)(x_1 - x_9)(x_1 - x_{11})(x_2 - x_6)\ldots(x_3 - 1)\ldots(x_4 - 2)(x_4 - 3)\ldots(x_{13} - 3)$
When is f_G equal to zero?When any factor is (i.e. when a rule is violated)!

$f_G =$
$(x_1 - x_5)(x_1 - x_9)(x_1 - x_{11})(x_2 - x_6) \ldots (x_3 - 1) \ldots (x_4 - 2)(x_4 - 3) \ldots (x_{13} - 3)$
When is f_G equal to zero?When any factor is (i.e. when a rule is violated)!
When is f_G nonzero?

$f_G =$
$(x_1 - x_5)(x_1 - x_9)(x_1 - x_{11})(x_2 - x_6)\ldots(x_3 - 1)\ldots(x_4 - 2)(x_4 - 3)\ldots(x_{13} - 3)$
When is f_G equal to zero?When any factor is (i.e. when a rule is violated)!
When is f_G nonzero? When each factor is nonzero (i.e. when no rule is violated)!

$f_G =$
$(x_1 - x_5)(x_1 - x_9)(x_1 - x_{11})(x_2 - x_6)\ldots(x_3 - 1)\ldots(x_4 - 2)(x_4 - 3)\ldots(x_{13} - 3)$
When is f_G equal to zero?When any factor is (i.e. when a rule is violated)!
When is f_G nonzero? When each factor is nonzero (i.e. when no rule is violated)!
We seek nonzeros that belong to $A_1 \times \cdots \times A_{13}$, where $A_i = \{1, 2, 3, 4\}$ for $1 \leq i \leq 13$.

FUNdamental Theorem of Algebra

You know that a one variable polynomial over a field $\mathbb{F}$ can have at most as many zeros as its degree.

FUNdamental Theorem of Algebra

You know that a one variable polynomial over a field $\mathbb{F}$ can have at most as many zeros as its degree.

Example: $f(x) = x^2 - 1$ and the set $A = \{1, -1, 3\}$.

$f(3) \neq 0$

FUNdamental Theorem of Algebra

You know that a one variable polynomial over a field $\mathbb{F}$ can have at most as many zeros as its degree.
Example: $f(x) = x^2 - 1$ and the set $A = \{1, -1, 3\}$.
$f(3) \neq 0$

Lemma

Let $\mathbb{F}$ be an arbitrary field, and let $f = f(x)$ be a polynomial in $\mathbb{F}[x]$. Suppose the degree of f is t (thus the x^t coefficient of f is nonzero). Then, if A is a subset of $\mathbb{F}$ with $|A| > t$, there is an $a \in A$ so that

$$f(a) \neq 0.$$

Combinatorial Nullstellensatz

Example: $f(x_1, x_2) = (x_1 - 1)(x_2 - 1)$ and the set $A_1 = \{1, 2\}, A_2 = \{1, 2\}$.

Combinatorial Nullstellensatz

Example: $f(x_1, x_2) = (x_1 - 1)(x_2 - 1)$ and the set $A_1 = \{1, 2\}, A_2 = \{1, 2\}$. $f(2, 2) \neq 0$.

Combinatorial Nullstellensatz

Example: $f(x_1, x_2) = (x_1 - 1)(x_2 - 1)$ and the set $A_1 = \{1, 2\}, A_2 = \{1, 2\}$. $f(2, 2) \neq 0$.

Theorem

[Combinatorial Nullstellensatz, N. Alon 1999] Let $\mathbb{F}$ be an arbitrary field, and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. Suppose the degree $\deg(f)$ of f is $\sum_{i=1}^{n} t_i$, where each t_i is a nonnegative integer, and suppose the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is nonzero. Then, if $A_1, \ldots, A_n$ are subsets of $\mathbb{F}$ with $|A_i| > t_i$, there are $a_1 \in A_1, \ldots, a_n \in A_n$ so that $f(a_1, \ldots, a_n) \neq 0$.

Given a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$, define the *support of* f, Supp(f), as the set of all $(\alpha_1, \ldots, \alpha_n)$ such that the coefficient of $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ in f is nonzero. We say $(\alpha_1, \ldots, \alpha_n) \geq (\beta_1, \ldots, \beta_n)$ if $\alpha_i \geq \beta_i$ for all i; this gives us a partial ordering of the elements of Supp(f).

Schauz's Coefficient Formula

Theorem

[Coefficient Formula, U. Schauz 2008]
Let f be a polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ and let $f_{\alpha_1,\ldots,\alpha_n}$ denote the coefficient of $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ in f. Suppose that there is no greater element than $(\alpha_1, \ldots, \alpha_n)$ in Supp(f). Then for any sets $A_1, \ldots, A_n$ in $\mathbb{F}$ such that $|A_i| = \alpha_i + 1$ we have

$$f_{\alpha_1,\ldots,\alpha_n} = \sum_{(a_1,\ldots,a_n)\in A_1\times\cdots\times A_n} \frac{f(a_1,\ldots,a_n)}{N(a_1,\ldots,a_n)}, \tag{1}$$

where $N(a_1, \ldots, a_n) = \prod_{i=1}^{n} \prod_{b\in A_i\setminus\{a_i\}} (a_i - b)$.

Note that this is ‘backwards’ to how we usually think – here we find coefficients from values, not values from the coefficients.

Corollary

[Schauz's Non-uniqueness Theorem, U. Schauz 2008] If $f_{\alpha_1,\ldots,\alpha_n} = 0$, *then either* f *vanishes over* $A_1 \times \cdots \times A_n$ *or* f *has at least two nonzero values over* $A_1 \times \cdots \times A_n$.

Corollary

[Schauz's Non-uniqueness Theorem, U. Schauz 2008] If $f_{\alpha_1,\ldots,\alpha_n} = 0$, then either f vanishes over $A_1 \times \cdots \times A_n$ or f has at least two nonzero values over $A_1 \times \cdots \times A_n$.

PROOF: If f is nonzero for exactly one element $(a_1, \ldots, a_n) \in A_\times \cdots \times A_n$, Equation 1 becomes $f_{\alpha_1,\ldots,\alpha_n} = \frac{f(a_1,\ldots,a_n)}{N(a_1,\ldots,a_n)} \neq 0$, as all other terms in the sum are zero.□

Corollary

[U. Schauz 2008] Let $\mathbb{F}$ be an arbitrary field, and let f be a polynomial of degree d in $\mathbb{F}[x_1, \ldots, x_n]$. Then for any subsets $A_1, \ldots, A_n$ of $\mathbb{F}$ satisfying $\sum_{i=1}^{n}(|A_i| - 1) > d$, f either vanishes over $A_1 \times \cdots \times A_n$ or f has at least two nonzero values over $A_1 \times \cdots \times A_n$.

Corollary

[U. Schauz 2008] Let $\mathbb{F}$ be an arbitrary field, and let f be a polynomial of degree d in $\mathbb{F}[x_1, \ldots, x_n]$. Then for any subsets $A_1, \ldots, A_n$ of $\mathbb{F}$ satisfying $\sum_{i=1}^{n}(|A_i| - 1) > d$, f either vanishes over $A_1 \times \cdots \times A_n$ or f has at least two nonzero values over $A_1 \times \cdots \times A_n$.

PROOF: Consider the monomial $x_1^{|A_1|-1} \cdots x_n^{|A_n|-1}$ in f. This is a monomial of degree greater than d, so its coefficient is zero. Applying the Non-uniqueness Theorem the conclusion follows immediately. $\square$

Corollary

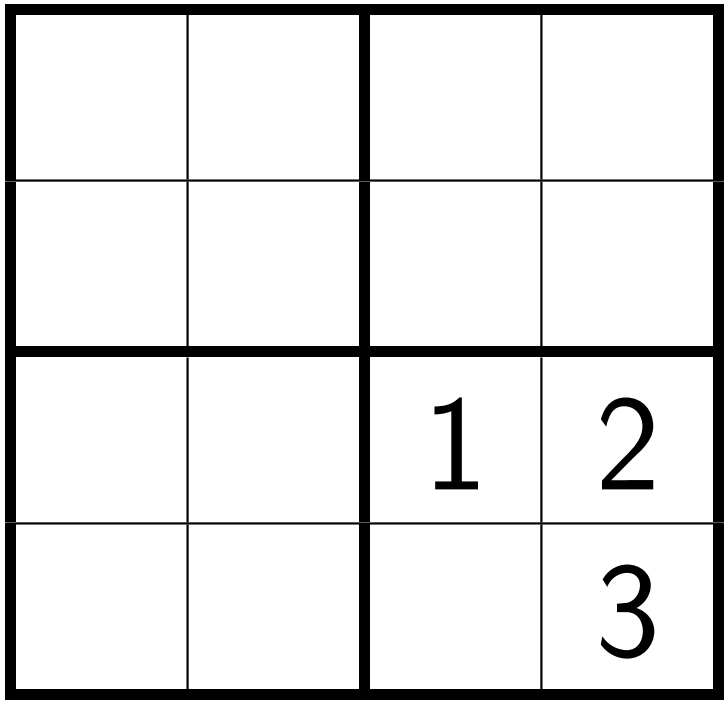
[U. Schauz 2008] Let $\mathbb{F}$ be an arbitrary field, and let f be a polynomial of degree d in $\mathbb{F}[x_1, \ldots, x_n]$. Then for any subsets $A_1, \ldots, A_n$ of $\mathbb{F}$ satisfying $\sum_{i=1}^{n}(|A_i| - 1) > d$, f either vanishes over $A_1 \times \cdots \times A_n$ or f has at least two nonzero values over $A_1 \times \cdots \times A_n$.

PROOF: Consider the monomial $x_1^{|A_1|-1} \cdots x_n^{|A_n|-1}$ in f. This is a monomial of degree greater than d, so its coefficient is zero. Applying the Non-uniqueness Theorem the conclusion follows immediately. $\square$

If the degree of the polynomial is small relative to the set we look over, then there cannot be a unique nonzero value.

Proof that one needs 4 clues in a Shidoku puzzle:
Only need to consider 3−clue puzzles with 3 distinct labels.

Proof that one needs 4 clues in a Shidoku puzzle:
Only need to consider 3−clue puzzles with 3 distinct labels.



PROOF THAT ONE NEEDS 4 CLUES IN A SHIDOKU PUZZLE:
Only need to consider 3−clue puzzles with 3 distinct labels.

x_1	x_2	x_3	x_4
x_5	x_6	x_7	x_8
x_9	x_{10}	1	2
x_{11}	x_{12}	x_{13}	3

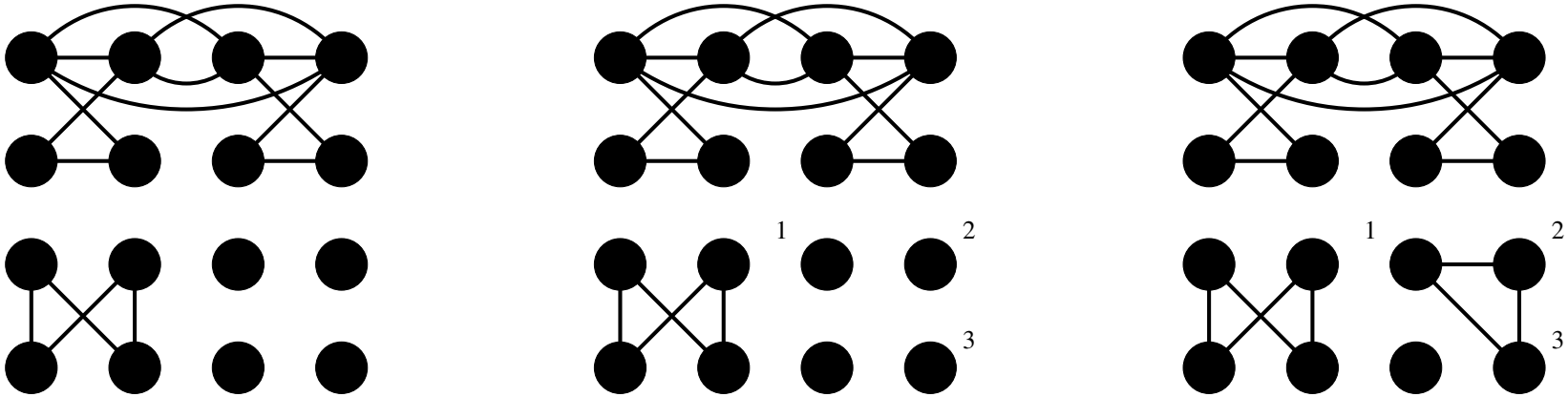


Figure : L-to-R: G_7; and with clues; and more edges deleted

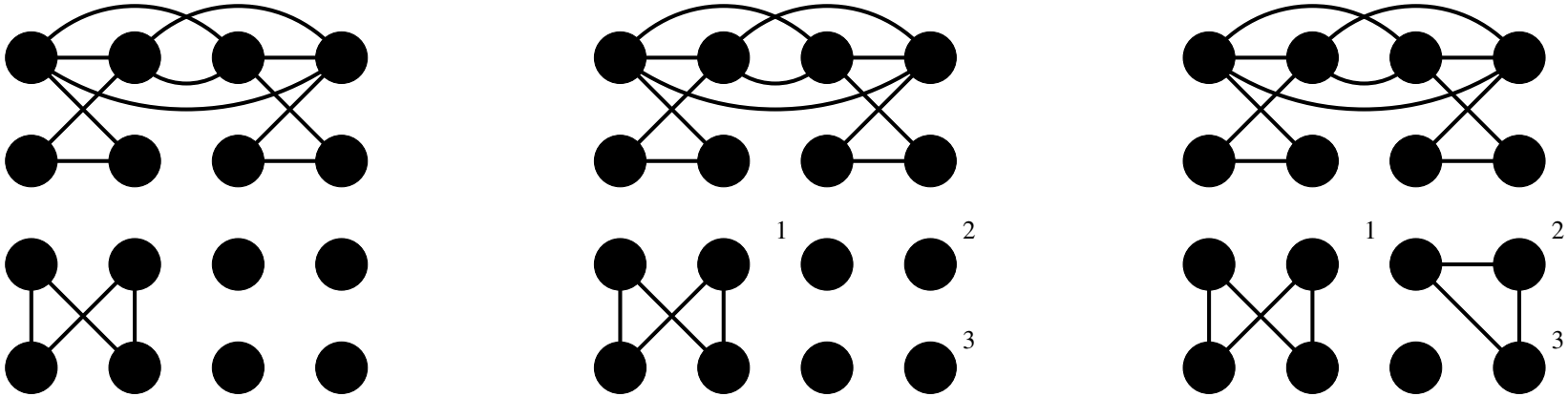
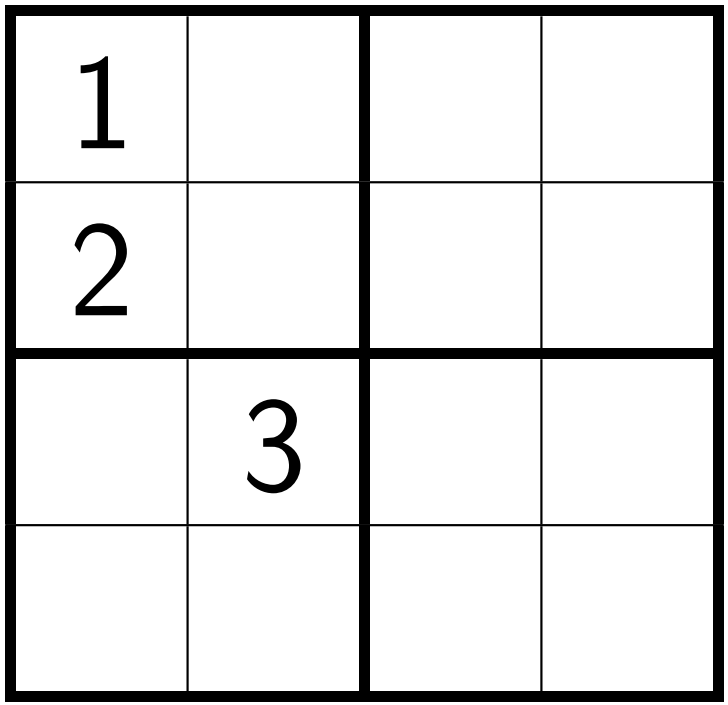


Figure : L-to-R: G_7; and with clues; and more edges deleted

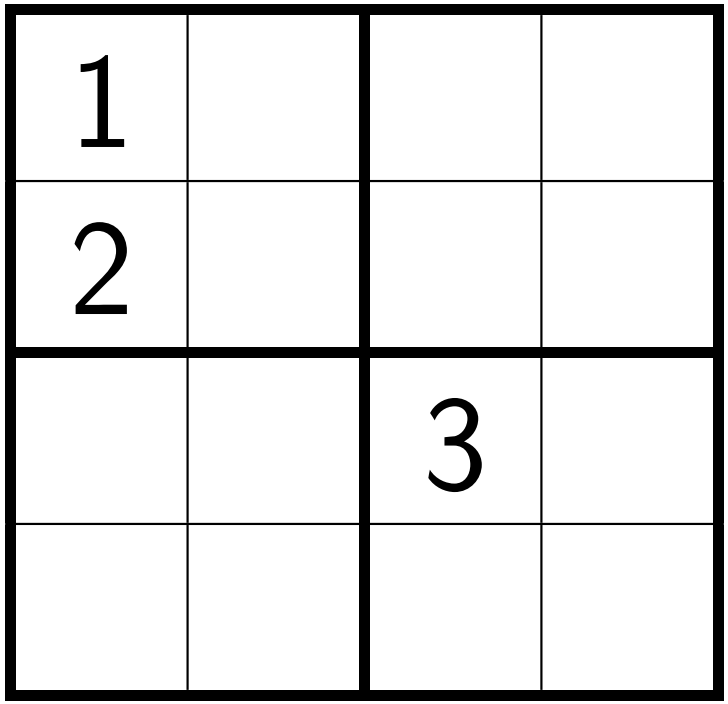
Consider, $f_G =$
$(x_1-x_5)(x_1-x_9)(x_1-x_{11})(x_2-x_6)\dots(x_3-1)\dots(x_4-2)(x_4-3)\dots(x_{13}-3)$.
Since the degree of f_G is small enough, i.e. $13 \cdot 3 > 37$, we apply the second corollary. So, f_G either vanishes over $A_1 \times \cdots \times A_{13}$ or f_G has at least two nonzero values over $A_1 \times \cdots \times A_{13}$. That is, we have no completion or multiple completions!

We argue similarly when there are three clues in the same box; three in the same row/column; two in the same box or in the same row/column and the third in the same column/row as one of the first two. (This case corresponds to the existence of at least two edges "between" clues that may be dropped.)
In each instance, we apply an appropriate symmetry of G_7. For each instance, there are at least two edges "between" clues that are not in the model and may be dropped. We obtain a polynomial with 13 variables and of degree at most $40 - 2 = 38$. We apply the second corollary and we are done.

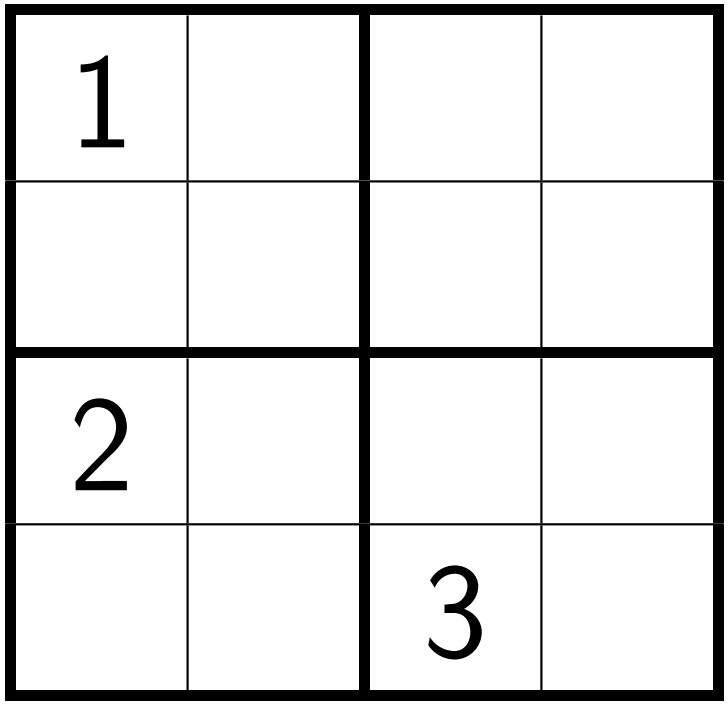
There are five cases with three distinct clues with at most one edge between them, up to isomorphism (and with an accompanying board) these are:
(1) two clues in the same row/column and box, with third clue in same chute as first two;



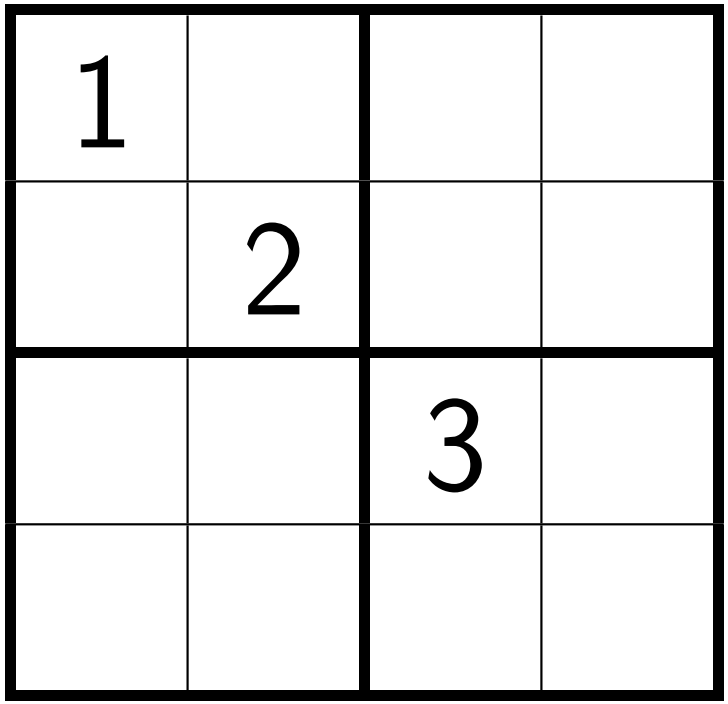
(2) two clues in the same row/column and box, with third clue in a different chute to the first two;



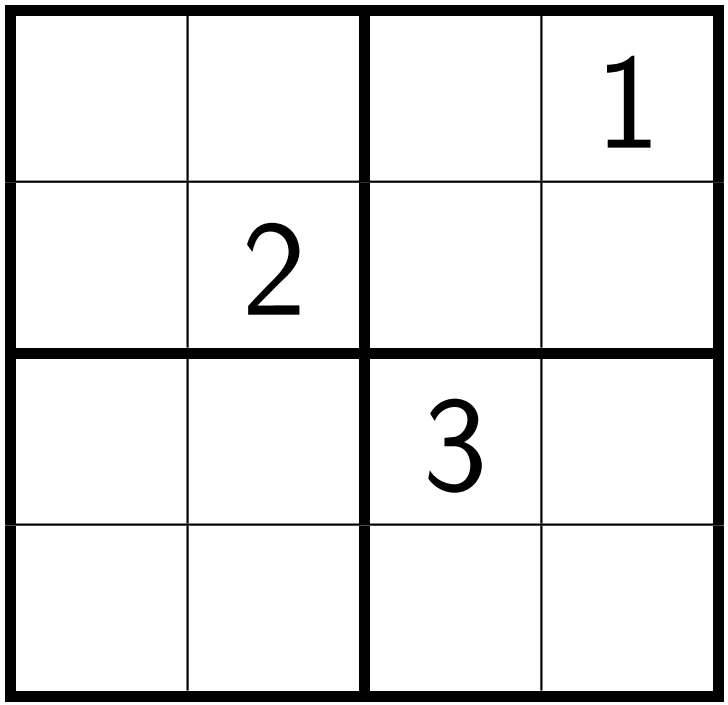
(3) two clues in the same row/column, different box;



(4) two clues in the same box, different row/column;



and, (5) no two clues in the same row, column, or box.



Case (2): we complete the first column uniquely and apply a 90-degree clockwise-rotation of model G_7.

1	x_1	x_2	x_3
2	x_4	x_5	x_6
4	x_7	**3**	x_8
3	x_9	x_{10}	x_{11}

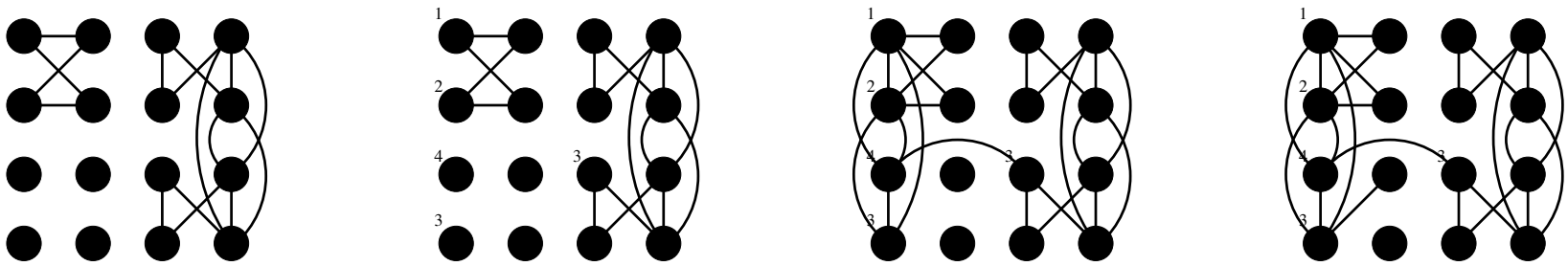


Figure : L-to-R: G_7 rotated 90-degrees clockwise; and with clues; and more edges deleted; yet more edges deleted

Delete the 24 edges contained in right-most graph from SUD_2; obtain a graph G with 56-24=32 edges.

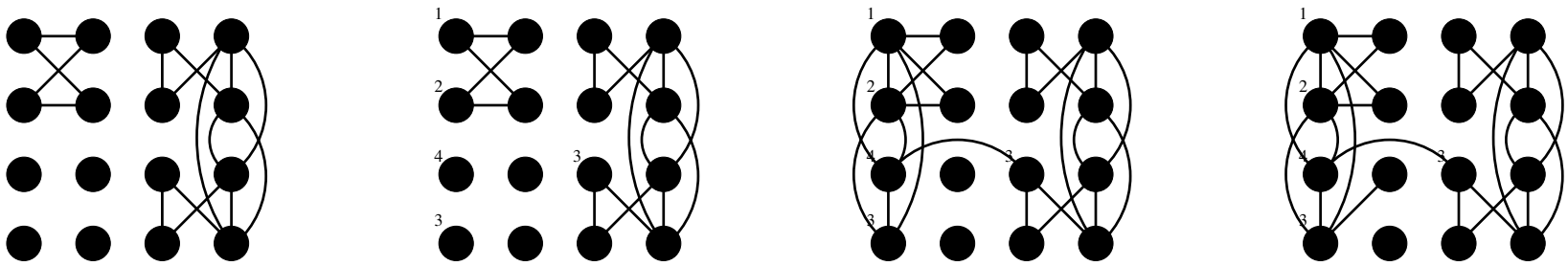


Figure : L-to-R: G_7 rotated 90-degrees clockwise; and with clues; and more edges deleted; yet more edges deleted

Delete the 24 edges contained in right-most graph from SUD_2; obtain a graph G with 56-24=32 edges.
Write down the *graph polynomial* f_G of the resulting graph:

$$f_G = f_G(x_1, \ldots, x_{11}) \in \mathbb{R}[x_1, \ldots, x_{11}].$$

Since the degree of f_G is small enough, i.e. $11 \cdot 3 > 32$, we apply the second corollary. So, f_G either vanishes over $A_1 \times \cdots \times A_{11}$ or f_G has at least two nonzero values over $A_1 \times \cdots \times A_{11}$.

Case (5): we complete the second row, third column, and upper-right box uniquely and apply a 180-degree clockwise rotation of model G_2. We delete 16 edges between the known clues, none of which are present in the model. We now have 8 variables and $40 - 16 = 24$ edges. As the degree of f_G is 24, we know that there is no greater element than the 8-length exponent vector of the form $(3, 3, \ldots, 3)$ in $Supp(f)$. To show that the coefficient of the monomial that corresponds to this exponent vector is zero, we give a visual proof.

		2	**1**
1	**2**	4	3
		3	
		1	

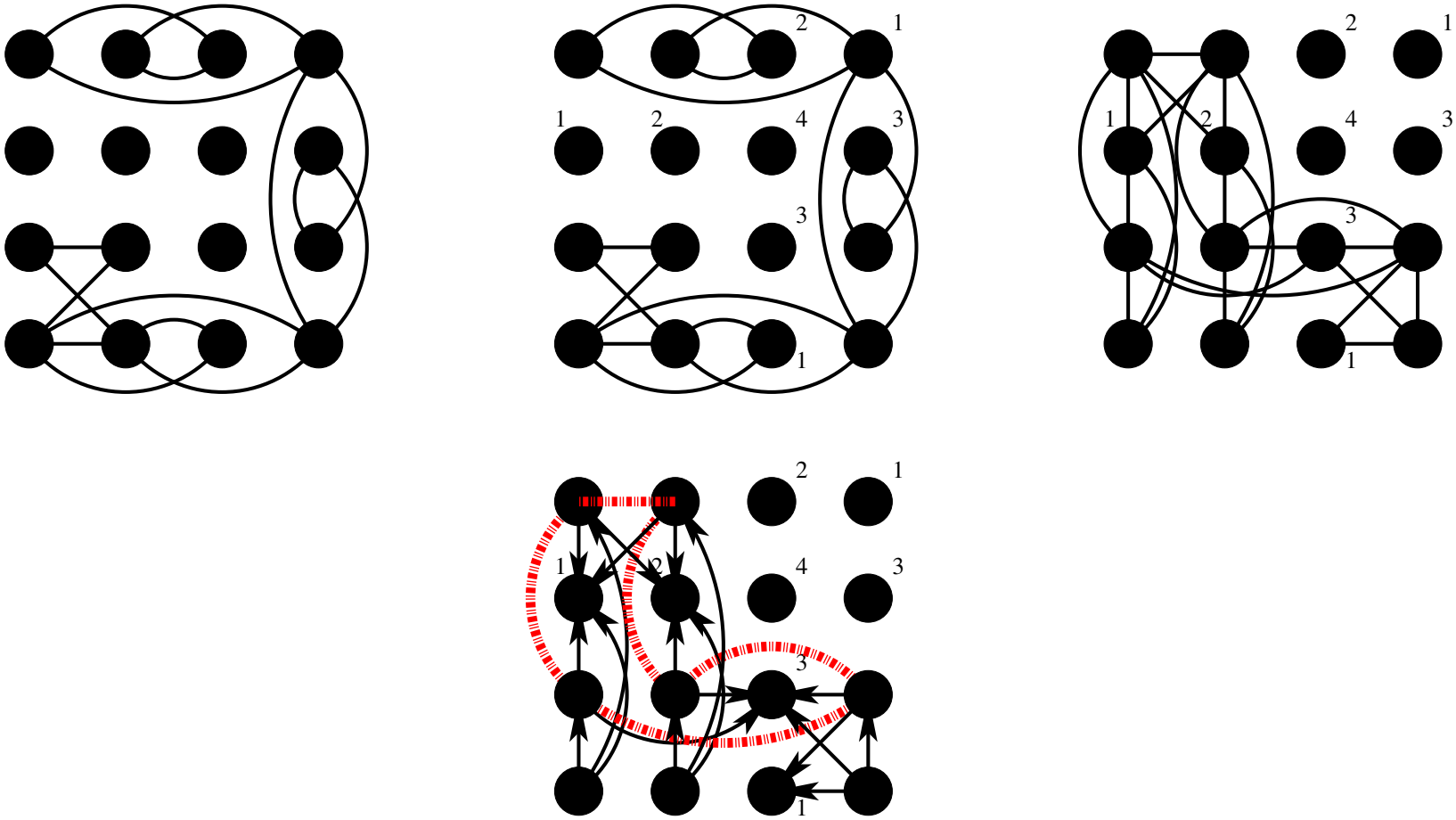


Figure : From left to right: G_2 rotated 180 degrees; and with the labeling; the built graph; and desired orientations of built graph

The polynomial method turns combinatorial problems into algebraic ones – it is often useful in providing lower bounds concerning cardinalities of sets.

The polynomial method turns combinatorial problems into algebraic ones – it is often useful in providing lower bounds concerning cardinalities of sets.

Question Might this approach allow for a computational approach that takes less than a full year of highly parallelized computation?

Thanks!