Automated Reasoning for Experimental Mathematics Part II: the Erdős Discrepancy Conjecture

Alexei Lisitsa[1]

[1] Department of Computer Science, The University of Liverpool

27 June 2019

Outline

- Part I: Automated Reasoning for Knots (computational topology)
- **Part II: Solution for the Erdős Discrepancy Problem, C=2 (combinatorial number theory)**
- Part III: Exploration of the Andrews-Curtis Conjecture (computational combinatorial group theory)

Part II is based on

(KL2014) Boris Konev, Alexei Lisitsa: A SAT Attack on the Erdős Discrepancy Conjecture. SAT 2014: 219-226

(KL2015) Boris Konev, Alexei Lisitsa: Computer-aided proof of Erdős discrepancy properties. Artif. Intell. 224: 103-118 (2015)

A very short version

The Erdős discrepancy conjecture is interesting (even for $C = 2$).

EDP2 can be settled by reduction to SAT.

A very short version

The Erdős discrepancy conjecture is interesting (even for $C = 2$).
EDP2 can be settled by reduction to SAT.

Longer version

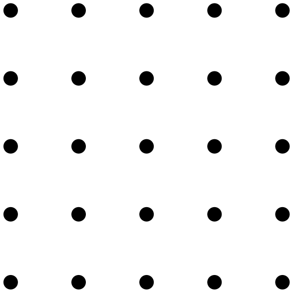
The Erdős discrepancy conjecture is interesting (even for $C = 2$).
EDP2 can be settled by reduction to SAT.

- Discrepancy Theory
- Erdős Discrepancy Conjecture
- SAT attack on the EDP
- Results and Perspectives

Discrepancy theory

Discrepancy theory is a branch of mathematics dealing with
inevitable irregularities of distributions

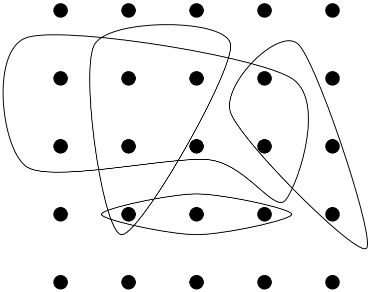
Combinatorial discrepancy



- A set U
- Set of subsets S

- A hypergraph $\mathcal{H} = (U, S)$
- Consider a colouring $c : U \to \{+1, -1\}$ of the elements of U in *blue* $(+1)$ and *red* (-1) colours;
- **Question:** Is there a colouring such that in every element of S colours are distributed uniformly or a **discrepancy** of colours is always inevitable?

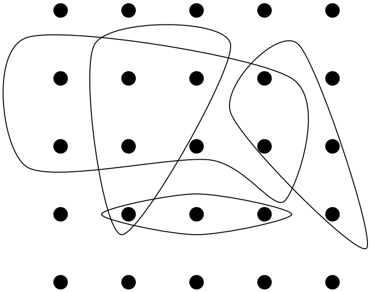
Combinatorial discrepancy



- A set U
- Set of subsets S

- A hypergraph $\mathcal{H} = (U, S)$
- Consider a colouring $c : U \to \{+1, -1\}$ of the elements of U in *blue* $(+1)$ and *red* (-1) colours;
- **Question:** Is there a colouring such that in every element of S colours are distributed uniformly or a **discrepancy** of colours is always inevitable?

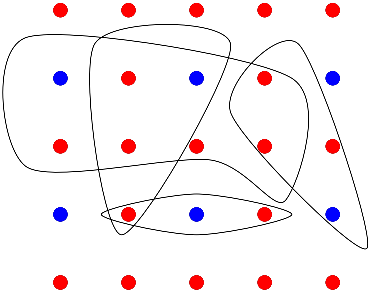
Combinatorial discrepancy



- A set U
- Set of subsets S

- A hypergraph $\mathcal{H} = (U, S)$
- Consider a colouring $c : U \to \{+1, -1\}$ of the elements of U in *blue* $(+1)$ and *red* (-1) colours;
- **Question:** Is there a colouring such that in every element of S colours are distributed uniformly or a **discrepancy** of colours is always inevitable?

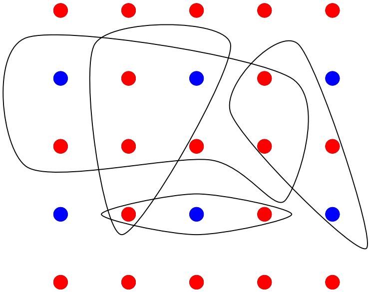
Combinatorial discrepancy



- A set U
- Set of subsets S

- A hypergraph $\mathcal{H} = (U, S)$
- Consider a colouring $c : U \to \{+1, -1\}$ of the elements of U in *blue* $(+1)$ and *red* (-1) colours;
- **Question:** Is there a colouring such that in every element of S colours are distributed uniformly or a **discrepancy** of colours is always inevitable?

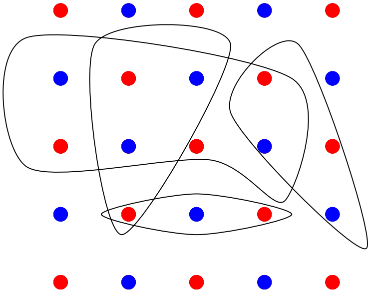
Combinatorial discrepancy



- A set U
- Set of subsets S

- A hypergraph $\mathcal{H} = (U, S)$
- Consider a colouring $c : U \to \{+1, -1\}$ of the elements of U in *blue* $(+1)$ and *red* (-1) colours;
- **Question:** Is there a colouring such that in every element of S colours are distributed uniformly or a **discrepancy** of colours is always inevitable?

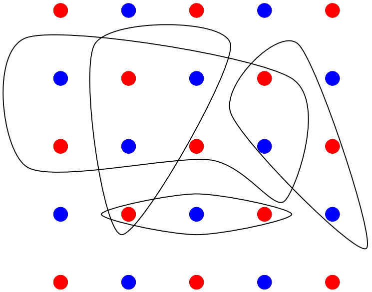
Combinatorial discrepancy



- A set U
- Set of subsets S

- A hypergraph $\mathcal{H} = (U, S)$
- Consider a colouring $c : U \to \{+1, -1\}$ of the elements of U in *blue* $(+1)$ and *red* (-1) colours;
- **Question:** Is there a colouring such that in every element of S colours are distributed uniformly or a **discrepancy** of colours is always inevitable?

Combinatorial discrepancy



- A set U
- Set of subsets S

$d(\mathcal{H}) = 1$

- A hypergraph $\mathcal{H} = (U, S)$
- Consider a colouring $c : U \to \{+1, -1\}$ of the elements of U in *blue* $(+1)$ and *red* (-1) colours;
- **Question:** Is there a colouring such that in every element of S colours are distributed uniformly or a **discrepancy** of colours is always inevitable?

Combinatorial number theory

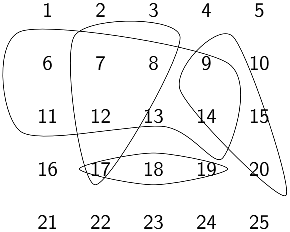
1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

- $U \subseteq \mathbb{N}$
- S — 'arithmetically interesting' subsets of U

Theorem (Roth, 1964)

For $U_n = \{1, 2, \ldots, n\}$ and $S_n = \{(a \cdot i + b)\}$ the discrepancy grows at least as $\frac{1}{20} n^{1/4}$.

Combinatorial number theory

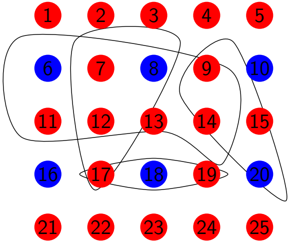


- $U \subseteq \mathbb{N}$
- S — 'arithmetically interesting' subsets of U

Theorem (Roth, 1964)

For $U_n = \{1, 2, \ldots, n\}$ and $S_n = \{(a \cdot i + b)\}$ the discrepancy grows at least as $\frac{1}{20}n^{1/4}$.

Combinatorial number theory

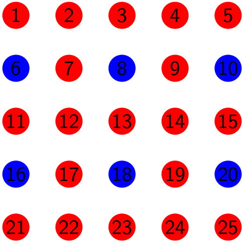


- $U \subseteq \mathbb{N}$
- S — 'arithmetically interesting' subsets of U

Theorem (Roth, 1964)

For $U_n = \{1, 2, \ldots, n\}$ and $S_n = \{(a \cdot i + b)\}$ the discrepancy grows at least as $\frac{1}{20} n^{1/4}$.

Combinatorial number theory



- $U \subseteq \mathbb{N}$
- S — 'arithmetically interesting' subsets of U

Theorem (Roth, 1964)

For $U_n = \{1, 2, \ldots, n\}$ and $S_n = \{(a \cdot i + b)\}$ the discrepancy grows at least as $\frac{1}{20} n^{1/4}$.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

What about **homogeneous** arithmetic progressions?

$$U_n = \{1, 2, \ldots, n\}$$

$$S_n = \{(a \cdot i)\}$$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

Erdős Discrepancy Conjecture (EDP)

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

What about **homogeneous** arithmetic progressions?

$$U_n = \{1, 2, \ldots, n\}$$

$$S_n = \{(a \cdot i)\}$$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

Erdős Discrepancy Conjecture (EDP)

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

What about **homogeneous** arithmetic progressions?

$$U_n = \{1, 2, \ldots, n\}$$

$$S_n = \{(a \cdot i)\}$$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

Known results on the discrepancy of $+1$ -1 sequences

- For random ± 1 sequences the discrepancy grows as $n^{1/2+o(1)}$ (folklore?);
- An explicit constructions of a sequence with slowly growing discrepancy $\log_3 n$ [Borwein, Choi, Coons, 2010];
- EDP holds for $C = 1$. [Mathias,1994]

Known results on the discrepancy of $+1$ -1 sequences

- For random ± 1 sequences the discrepancy grows as $n^{1/2+o(1)}$ (folklore?);
- An explicit constructions of a sequence with slowly growing discrepancy $\log_3 n$ [Borwein, Choi, Coons, 2010];
- EDP holds for $C = 1$. [Mathias,1994]

Known results on the discrepancy of $+1$ -1 sequences

- For random ± 1 sequences the discrepancy grows as $n^{1/2+o(1)}$ (folklore?);
- An explicit constructions of a sequence with slowly growing discrepancy $\log_3 n$ [Borwein, Choi, Coons, 2010];
- EDP holds for $C = 1$. [Mathias,1994]

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

–	–	–	–	–	–	–	–	–	–	–	–
1	2	3	4	5	6	7	8	9	10	11	12

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $\mid \sum_{i=1}^{k} x_{i \cdot d} \mid > C$.

+	_	_	_	_	_	_	_	_	_	_	_	$d = 1$
1	2	3	4	5	6	7	8	9	10	11	12	

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $| \sum_{i=1}^{k} x_{i \cdot d} | > C$.

+	+	_	_	_	_	_	_	_	_	_	_	$d = 1$
1	2	3	4	5	6	7	8	9	10	11	12	

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $| \sum_{i=1}^{k} x_{i \cdot d} | > C$.

+	+	–	–	–	–	–	–	–	–	–	–	$d = 1$
1	2	3	4	5	6	7	8	9	10	11	12	

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $\mid \sum_{i=1}^{k} x_{i \cdot d} \mid > C$.

+	−	_	_	_	_	_	_	_	_	_	_	$d = 1$
1	2	3	4	5	6	7	8	9	10	11	12	

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

+	−	_	+	_	_	_	_	_	_	_	_	$d = 2$
1	2	3	4	5	6	7	8	9	10	11	12	

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

+	−	−	+	_	_	_	_	_	_	_	_	$d = 1$
1	2	3	4	5	6	7	8	9	10	11	12	

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

+	−	−	+	_	+	_	_	_	_	_	_	$d = 3$
1	2	3	4	5	6	7	8	9	10	11	12	

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

+	−	−	+	−	+	_	_	_	_	_	_	$d = 1$
1	2	3	4	5	6	7	8	9	10	11	12	

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $\mid \sum_{i=1}^{k} x_{i \cdot d} \mid > C$.

+	−	−	+	−	+	_	−	_	_	_	_
1	2	3	4	5	6	7	8	9	10	11	12

$d = 4$

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

+	−	−	+	−	+	+	−	_	_	_	_	$d = 1$
1	2	3	4	5	6	7	8	9	10	11	12	

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

+	−	−	+	−	+	+	−	_	+	_	_	$d = 5$
1	2	3	4	5	6	7	8	9	10	11	12	

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

+	−	−	+	−	+	+	−	−	+	_	_	$d = 1$
1	2	3	4	5	6	7	8	9	10	11	12	

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

+	−	−	+	−	+	+	−	−	+	_	−	$d = 6$
1	2	3	4	5	6	7	8	9	10	11	12	

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $\mid \sum_{i=1}^{k} x_{i \cdot d} \mid > C$.

+	−	−	+	−	+	+	−	−	+	+	−	$d = 1$
1	2	3	4	5	6	7	8	9	10	11	12	

Example: $C = 1$

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

+	−	−	+	−	+	+	−	−	+	+	−	$d = 3$
1	2	3	4	5	6	7	8	9	10	11	12	

But then $x_3 + x_6 + x_9 + x_{12} = -1 + 1 - 1 - 1 = -2$

Polymath and the EDP

- A 2009-2010 topic of Polymath — ‘massively collaborative maths’ project started and coordinated by T. Gowers
  - A computer attack
  - Discrepancy 2 sequences of length 1124 (backtracking search)

“. . . given how long a finite sequence can be, it seems unlikely that we could answer this question just by a clever search of all possibilities on a computer. . . ”

Polymath and the EDP

- A 2009-2010 topic of Polymath — 'massively collaborative maths' project started and coordinated by T. Gowers
  - A computer attack
  - Discrepancy 2 sequences of length 1124 (backtracking search)

"...given how long a finite sequence can be, it seems unlikely that we could answer this question just by a clever search of all possibilities on a computer..."

Polymath and the EDP

- A 2009-2010 topic of Polymath — 'massively collaborative maths' project started and coordinated by T. Gowers
  - A computer attack
  - Discrepancy 2 sequences of length 1124 (backtracking search)

"...given how long a finite sequence can be, it seems unlikely that we could answer this question just by a clever search of all possibilities on a computer..."

Polymath and the EDP

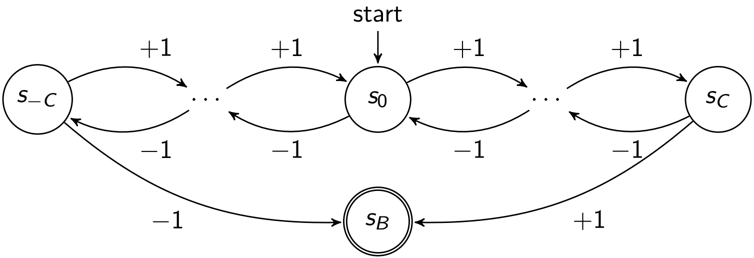
- A 2009-2010 topic of Polymath — 'massively collaborative maths' project started and coordinated by T. Gowers
  - A computer attack
  - Discrepancy 2 sequences of length 1124 (backtracking search)

"...given how long a finite sequence can be, it seems unlikely that we could answer this question just by a clever search of all possibilities on a computer..."

Our contribution

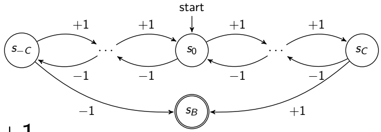
- There are ± 1 sequences of length 1160 and discrepancy 2,
- There are no ± 1 sequences of length 1161 (or more) and discrepancy 2.

Automata encoding of discrepancy conditions



- If for every $d : 1 \leq d \leq \lfloor \frac{n}{C+1} \rfloor$ the automaton $\mathcal{A}_C$ *does not* accept the subsequence $x_d, x_{2d}, \dots, x_{kd}$, where $k = \lfloor \frac{n}{d} \rfloor$ then the discrepancy of the sequence $\bar{x}$ does not exceed C

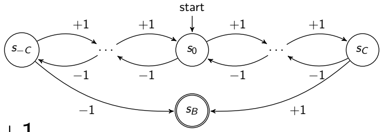
SAT representation



- p_i is true if $\iff$ i-th letter is $+1$.
- $s_j^{(i,d)}$ is true $\iff$ $\mathcal{A}_C$ is in s_j having read first $(i-1)$ letters.

$$\phi_{(n,C,d)} = s_0^{(1,d)} \bigwedge_{i=1}^{\lfloor \frac{n}{d} \rfloor} \Bigg[\bigwedge_{-C \leq j < C} \left(s_j^{(i,d)} \wedge p_{i \cdot d} \to s_{j+1}^{(i+1,d)} \right) \wedge \bigwedge_{-C < j \leq C} \left(s_j^{(i,d)} \wedge \neg p_{i \cdot d} \to s_{j-1}^{(i+1,d)} \right) \wedge \left(s_C^{(i,d)} \wedge p_{i \cdot d} \to B \right) \wedge \left(s_{-C}^{(i,d)} \wedge \neg p_{i \cdot d} \to B \right) \Bigg]$$

SAT representation



- p_i is true if $\iff$ i-th letter is $+1$.
- $s_j^{(i,d)}$ is true $\iff$ $\mathcal{A}_C$ is in s_j having read first $(i-1)$ letters.

$$\phi_{(n,C,d)} = s_0^{(1,d)} \bigwedge_{i=1}^{\lfloor \frac{n}{d} \rfloor} \Bigg[\begin{array}{l} \bigwedge_{-C \le j < C} \left(s_j^{(i,d)} \wedge p_{i \cdot d} \to s_{j+1}^{(i+1,d)} \right) \wedge \\ \bigwedge_{-C < j \le C} \left(s_j^{(i,d)} \wedge \neg p_{i \cdot d} \to s_{j-1}^{(i+1,d)} \right) \wedge \\ \left(s_C^{(i,d)} \wedge p_{i \cdot d} \to B \right) \wedge \\ \left(s_{-C}^{(i,d)} \wedge \neg p_{i \cdot d} \to B \right) \end{array} \Bigg]$$

Adequacy and correctness of encoding

Let

$$\phi_{(n,C)} = \neg B \wedge \bigwedge_{d=1}^{\lfloor \frac{n}{C+1} \rfloor} \phi_{(n,C,d)} \wedge \mathrm{frame}_{(n,C)},$$

where $\mathrm{frame}_{(n,C)}$ is a Boolean formula encoding that the automaton state is correctly defined.

Proposition

The formula $\phi_{(n,C)}$ is satisfiable if, and only if, there exists a ± 1 sequence $\bar{x} = x_1, \ldots, x_n$ of length n of discrepancy C. Moreover, if $\phi_{(n,C)}$ is satisfiable, the sequence $\bar{x} = x_1, \ldots, x_n$ of discrepancy C is uniquely identified by the assignment of truth values to propositions $p_1, \ldots p_n$.

Adequacy and correctness of encoding

Let

$$\phi_{(n,C)} = \neg B \wedge \bigwedge_{d=1}^{\lfloor \frac{n}{C+1} \rfloor} \phi_{(n,C,d)} \wedge \mathrm{frame}_{(n,C)},$$

where $\mathrm{frame}_{(n,C)}$ is a Boolean formula encoding that the automaton state is correctly defined.

Proposition

The formula $\phi_{(n,C)}$ is satisfiable if, and only if, there exists a ± 1 sequence $\bar{x} = x_1, \ldots, x_n$ of length n of discrepancy C. Moreover, if $\phi_{(n,C)}$ is satisfiable, the sequence $\bar{x} = x_1, \ldots, x_n$ of discrepancy C is uniquely identified by the assignment of truth values to propositions $p_1, \ldots p_n$.

Disclaimer

In fact we have used more "economical" encoding, where a state s_i of automaton is encoded not by a separate propositional variable p_i, but by the propositional variables encoding i in binary

Experiments and Results

In our experiments we used

- the Lingeling SAT solver, the winner of the *SAT-UNSAT* category of the SAT'13 competition, and
- the Glucose solver version, the winner of the *certified UNSAT* category of the SAT'13 competition.

All experiments were conducted on PCs equipped with an Intel Core i5-2500K CPU running at 3.30GHz and 16GB of RAM.

Experiments and Results

- By iteratively increasing the length of the sequence, we establish precisely that the maximal length of a ± 1 sequence of discrepancy 2 is 1160.
- On our system it took Plingeling, the parallel version of the Lingeling solver, about 800 seconds to generate a sequence of discrepancy 2 and length 1160.
- On the other hand, when we increased the length of the sequence to 1161, Plingeling reported unsatisfiability.
- We also used Glucose: It took the solver about 21 500 seconds to compute a Delete Reverse Unit Propagation (DRUP) certificate of unsatisfiability ($\sim$ 13Gb).
- The certificate has been independently verified by the drup-trim tool

Experiments and Results

- By iteratively increasing the length of the sequence, we establish precisely that the maximal length of a ± 1 sequence of discrepancy 2 is 1160.
- On our system it took Plingeling, the parallel version of the Lingeling solver, about 800 seconds to generate a sequence of discrepancy 2 and length 1160.
- On the other hand, when we increased the length of the sequence to 1161, Plingeling reported unsatisfiability.
- We also used Glucose: It took the solver about 21 500 seconds to compute a Delete Reverse Unit Propagation (DRUP) certificate of unsatisfiability ($\sim$ 13Gb).
- The certificate has been independently verified by the drup-trim tool

Experiments and Results

- By iteratively increasing the length of the sequence, we establish precisely that the maximal length of a ± 1 sequence of discrepancy 2 is 1160.
- On our system it took Plingeling, the parallel version of the Lingeling solver, about 800 seconds to generate a sequence of discrepancy 2 and length 1160.
- On the other hand, when we increased the length of the sequence to 1161, Plingeling reported unsatisfiability.
- We also used Glucose: It took the solver about 21 500 seconds to compute a Delete Reverse Unit Propagation (DRUP) certificate of unsatisfiability ($\sim$ 13Gb).
- The certificate has been independently verified by the drup-trim tool

EDP2 is done!

Theorem

Any ± 1 *sequence of length* 1161 *has discrepancy at least* 3.

Corollary

The Erdős discrepancy conjecture holds true for $C = 2$.

EDP2 is done!

Theorem

Any ± 1 *sequence of length* 1161 *has discrepancy at least* 3.

Corollary

The Erdős discrepancy conjecture holds true for $C = 2$.

Deep asymmetry

- It is easy to check, either by a simple program, or even by hands that a 1160 sequence has discrepancy 2;
- It is computationally difficult to obtain a certificate of unsatisfiability. It is even more difficult to come up with a human comprehensible proof;
  - 13GB!
- **Challenge**: Give a human understandable proof of non-existence of 1161 sequences of discrepancy 2.

Deep asymmetry

- It is easy to check, either by a simple program, or even by hands that a 1160 sequence has discrepancy 2;
- It is computationally difficult to obtain a certificate of unsatisfiability. It is even more difficult to come up with a human comprehensible proof;
  - 13GB!
- **Challenge**: Give a human understandable proof of non-existence of 1161 sequences of discrepancy 2.

Deep asymmetry

- It is easy to check, either by a simple program, or even by hands that a 1160 sequence has discrepancy 2;
- It is computationally difficult to obtain a certificate of unsatisfiability. It is even more difficult to come up with a human comprehensible proof;
  - 13GB!
- **Challenge**: Give a human understandable proof of non-existence of 1161 sequences of discrepancy 2.

EDP3 ?

We have applied the same methodology to the case C=3.

Proposition

There exists a sequence of length $\approx 14,000$ *of discrepancy* 3.

Life after SAT:

- Better SAT encodings
- Tuned search strategy
- 850Mb RUP certificate for EDP2

Life after SAT: Journal submission, CoRR abs/1405.3097

- Better SAT encodings
- Tuned search strategy
- 850Mb RUP certificate for EDP2
- Multiplicative and completely multiplicative sequences for EDP3

$$x_{m \cdot n} = x_m \cdot x_n$$

- Longest completely multiplicative EDP3 sequences contains 127 645 elements
  - (independently reported by Le Bras, Gomes and Selman, CoRR abs/1407.2510)
- Longest multiplicative EDP3 sequences also contains 127 645 elements!
  - Not so for $C = 1$ and $C = 2$
- New lower bound for EDP3 of **130 000**

Life after SAT: Journal submission, CoRR abs/1405.3097

- Better SAT encodings
- Tuned search strategy
- 850Mb RUP certificate for EDP2
- Multiplicative and completely multiplicative sequences for EDP3

$$x_{m \cdot n} = x_m \cdot x_n$$

- Longest completely multiplicative EDP3 sequences contains 127 645 elements
  - (independently reported by La Bras, Gomes and Selman, CoRR abs/1407.2510)
- Longest multiplicative EDP3 sequences also contains 127 645 elements!
  - Not so for $C = 1$ and $C = 2$
- New lower bound for EDP3 of **130 000**

Life after SAT: Journal submission, CoRR abs/1405.3097

- Better SAT encodings
- Tuned search strategy
- 850Mb RUP certificate for EDP2
- Multiplicative and completely multiplicative sequences for EDP3

$$x_{m \cdot n} = x_m \cdot x_n$$

- Longest completely multiplicative EDP3 sequences contains 127 645 elements
  - (independently reported by La Bras, Gomes and Selman, CoRR abs/1407.2510)
- Longest multiplicative EDP3 sequences also contains 127 645 elements!
  - Not so for $C = 1$ and $C = 2$
- New lower bound for EDP3 of **130 000**

Life after SAT: Journal submission, CoRR abs/1405.3097

- Better SAT encodings
- Tuned search strategy
- 850Mb RUP certificate for EDP2
- Multiplicative and completely multiplicative sequences for EDP3

$$x_{m \cdot n} = x_m \cdot x_n$$

- Longest completely multiplicative EDP3 sequences contains 127 645 elements
  - (independently reported by La Bras, Gomes and Selman, CoRR abs/1407.2510)
- Longest multiplicative EDP3 sequences also contains 127 645 elements!
  - Not so for $C = 1$ and $C = 2$
- New lower bound for EDP3 of **130 000**

Life after SAT: Journal submission, CoRR abs/1405.3097

- Better SAT encodings
- Tuned search strategy
- 850Mb RUP certificate for EDP2
- Multiplicative and completely multiplicative sequences for EDP3

$$x_{m \cdot n} = x_m \cdot x_n$$

- Longest completely multiplicative EDP3 sequences contains 127 645 elements
  - (independently reported by La Bras, Gomes and Selman, CoRR abs/1407.2510)
- Longest multiplicative EDP3 sequences also contains 127 645 elements!
  - Not so for $C = 1$ and $C = 2$
- New lower bound for EDP3 of **130 000**

- Better SAT encodings
- Tuned search strategy
- 850Mb RUP certificate for EDP2
- Multiplicative and completely multiplicative sequences for EDP3

$$x_{m \cdot n} = x_m \cdot x_n$$

- Longest completely multiplicative EDP3 sequences contains 127 645 elements
  - (independently reported by La Bras, Gomes and Selman, CoRR abs/1407.2510)
- Longest multiplicative EDP3 sequences also contains 127 645 elements!
  - Not so for $C = 1$ and $C = 2$
- New lower bound for EDP3 of **130 000**

Life after SAT, 2015

Terence Tao, September 2015

Proof of general case of EDP.

Conjecture (Erdős, circa 1930)

For any $C > 0$ in any infinite ± 1 sequence (x_n) there exists a subsequence $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ such that $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

Not SAT solving or automated reasoning, but full power of Fields prize laureate's mind!

Terence Tao, September 2015
Proof of general case of EDP.

Conjecture (Erdős, circa 1930)

For any $C > 0$ *in any infinite* ± 1 *sequence* (x_n) *there exists a subsequence* $x_d, x_{2d}, x_{3d}, \ldots, x_{kd}$ *such that* $|\sum_{i=1}^{k} x_{i \cdot d}| > C$.

Not SAT solving or automated reasoning, but full power of Fields prize laureate's mind!

Conclusion

- Another example of the power of SAT
  - Outperforms bespoke tools
- Reignited the debate on what a mathematical proof is
- Further development
- **Challenge**: Give a human understandable proof of EDP2, EDP3, ...
  - EDP

Conclusion

- Another example of the power of SAT
  - Outperforms bespoke tools
- Reignited the debate on what a mathematical proof is
- Further development
- **Challenge**: Give a human understandable proof of EDP2, EDP3, . . .
  - EDP

Conclusion

- Another example of the power of SAT
  - Outperforms bespoke tools
- Reignited the debate on what a mathematical proof is
- Further development
- **Challenge**: Give a human understandable proof of EDP2, EDP3, ...
  - EDP

Conclusion

- Another example of the power of SAT
  - Outperforms bespoke tools
- Reignited the debate on what a mathematical proof is
- Further development
- **Challenge**: Give a human understandable proof of EDP2, EDP3, . . .
  - EDP

Conclusion

- Another example of the power of SAT
  - Outperforms bespoke tools
- Reignited the debate on what a mathematical proof is
- Further development
- **Challenge**: Give a human understandable proof of EDP2, EDP3, . . .
  - EDP

Conclusion

- Another example of the power of SAT
  - Outperforms bespoke tools
- Reignited the debate on what a mathematical proof is
- Further development
- **Challenge**: Give a human understandable proof of EDP2, EDP3, . . .
  - EDP

Conclusion

- Another example of the power of SAT
  - Outperforms bespoke tools
- Reignited the debate on what a mathematical proof is
- Further development
- **Challenge**: Give a human understandable proof of EDP2, EDP3, ...
  - EDP

A sequence of length 1160 and discrepancy 2

```
− + + − + − − + + − + + − + − − + − − + + − + − − + − − + + − + − − + + − + + −
+ − + + − − + + − + − − − + − + + − + − − + − − + + + + − − + − − + + − + − − +
+ − + + − − − − + + − + + − + − + + − − + + − + − + − − − + + − + − − + + − + +
− + − − + + − + − − + − − − + − + + − + − − + + − + + − + − − + − − + + − + + −
+ − − + + − + − − + + + − + − + − − − − + + + − + − − + − − + + + − − − + + − +
+ − + − − + − − + + + − − + − + − + − − + − + + + − + + − + − − + − − + + − + −
− + + − + + − + − − + − − + + − − + + + − − − + + + − + − − − + + − + − − + + −
− + − + − − + − + + + − + − − + + − + + − + − − + + − + − − + − − + + − + − − +
+ − − + − + + − + − + − − + − + − + + − + − − + + − + − − + − − + + − + − + − +
+ − + − + − + + − − − + − + − − + + + + − − + − − − + + − + − + + − + − − + + −
+ − − + − − + + − + − − + + + + − − + − − − + − + + + + − − + − − + + − + + − +
− − + + − + − − + − − + + − + − − + + − + + − + − − + + − + − − + − − + + − + +
− + − − − − + + + − + − − + + − − + + + − − − + − + + − + − − + − + + − − − + −
+ + − + + − + − − + − − + + − − + + + + − + − − + − − + − − + + + + − − + − − +
+ + − − − + + − + + − + − − + + − − + − + − − + − − + + − + + − + − − + − − + −
+ + + − + + − + − − + − − + + − − + − + + − + + − + − − + − − + − − + + − + + −
+ − − + + + − − − + + − + − − + + − + + − − − + + + − − − + + − + + − − − − + +
+ − − + − + + − + − − + − − + + − + − − + + − + + − + − + + − − + + − − + + − −
− − + + + − + + − − + + − − − − + + − + + + − − + + − − − + + + − − − − + − + −
+ + − + + − + + − + − + − − − − + + + − − + + − + − − + + − + + − + − − + − − +
− − + + − + − − + + − + + − + − − + + − − + − + − − + − + − + − + + + + − − − +
− + − + + − − + − − + − + − + − + + − + − + + + − − + − + − − + − − + − + + + −
− + − + + + − − − + + − + − − + − − + + − + + − − + + − − − + + − + − + + − − +
+ − + − − − + − + + − + − − + − + + − − + + − + − − + + − + − − + − + + + − + −
− + + − − + − + − + + + − − + − + − − + + − + + − + − − + − − + − + + − − − + −
+ + − + − + + − − + + − + − − + + + − + − − − − + + − − + − + + − + − + + − − +
+ − + − − + + − + − + + − − + + − + − − − + − + + − + − − + + + − − − − + − + −
+ + − − + + − + − − + + − + + − + + − + − − + − − + − − + + + + − − − + + − − −
+ − + − + + − + − + + + − − + − + + − − + − + − − + − + − + + − − − + + + − + +
```