Hard Combinatorial Problems: A Challenge for Satisfiability

Ilias S. Kotsireas[1]

[1]Director, CARGO Lab
http://www.cargo.wlu.ca
Wilfrid Laurier University, Waterloo ON, Canada

Joint work with Curtis Bright, Albert Heinle, Vijay Ganesh

SC^2 2018, http://www.sc-square.org/
Satisfiability Checking and Symbolic Computation
11th July 2018, Oxford, United Kingdom, Part of FLoC 2018

Talk Outline

1. Autocorrelation
2. Complementary Sequences
3. Hard Combinatorial Problems via Autocorrelation
4. SAT encodings of Autocorrelation
5. MathCheck
   https://sites.google.com/site/uwmathcheck
6. The new petaflop Canadian HPC landscape
7. Other significant Hard Combinatorial Problems
8. On-going and future work

Autocorrelation of finite sequences

Autocorrelation of finite sequences

- The **periodic autocorrelation function** associated to a finite sequence $A = [a_0, \ldots, a_{n-1}]$ of length n is defined as

$$P_A(s) = \sum_{k=0}^{n-1} a_k a_{k+s}, \;\; s = 0, \ldots, n-1,$$

where $k + s$ is taken modulo n, when $k + s \geq n$.

Autocorrelation of finite sequences

- The **periodic autocorrelation function** associated to a finite sequence $A = [a_0, \ldots, a_{n-1}]$ of length n is defined as

$$P_A(s) = \sum_{k=0}^{n-1} a_k a_{k+s}, \ \ s = 0, \ldots, n-1,$$

where $k + s$ is taken modulo n, when $k + s \geq n$.

- The **aperiodic autocorrelation function** associated to a finite sequence $A = [a_0, \ldots, a_{n-1}]$ of length n is defined as

$$N_A(s) = \sum_{k=0}^{n-1-s} a_k a_{k+s}, \ \ s = 0, \ldots, n-1,$$

Autocorrelation of finite sequences

- The **periodic autocorrelation function** associated to a finite sequence $A = [a_0, \ldots, a_{n-1}]$ of length n is defined as

$$P_A(s) = \sum_{k=0}^{n-1} a_k a_{k+s}, \; s = 0, \ldots, n-1,$$

  where $k + s$ is taken modulo n, when $k + s \geq n$.
- The **aperiodic autocorrelation function** associated to a finite sequence $A = [a_0, \ldots, a_{n-1}]$ of length n is defined as

$$N_A(s) = \sum_{k=0}^{n-1-s} a_k a_{k+s}, \; s = 0, \ldots, n-1,$$

- We are mostly concerned with binary $\{-1, +1\}$, ternary $\{-1, 0, +1\}$ and 4-th roots of unity $\{\pm 1, \pm i\}$ sequences.

Autocorrelation of finite sequences

- The **periodic autocorrelation function** associated to a finite sequence $A = [a_0, \ldots, a_{n-1}]$ of length n is defined as

$$P_A(s) = \sum_{k=0}^{n-1} a_k a_{k+s}, \; s = 0, \ldots, n-1,$$

where $k + s$ is taken modulo n, when $k + s \geq n$.
- The **aperiodic autocorrelation function** associated to a finite sequence $A = [a_0, \ldots, a_{n-1}]$ of length n is defined as

$$N_A(s) = \sum_{k=0}^{n-1-s} a_k a_{k+s}, \; s = 0, \ldots, n-1,$$

- We are mostly concerned with binary $\{-1, +1\}$, ternary $\{-1, 0, +1\}$ and 4-th roots of unity $\{\pm 1, \pm i\}$ sequences.
- For sequences with complex number elements, a_{k+s} is replaced by $\overline{a_{k+s}}$.

Example: $n = 7$, $A = [a_1, \ldots, a_7]$

Example: $n = 7$, $A = [a_1, \ldots, a_7]$

$$\begin{array}{lcl}
P_A(0) & = & {a_1}^2 + {a_2}^2 + {a_3}^2 + {a_4}^2 + {a_5}^2 + {a_6}^2 + {a_7}^2 \\
P_A(1) & = & a_1 a_2 + a_2 a_3 + a_3 a_4 + a_4 a_5 + a_5 a_6 + a_6 a_7 + a_7 a_1 \\
P_A(2) & = & a_1 a_3 + a_2 a_4 + a_3 a_5 + a_4 a_6 + a_5 a_7 + a_6 a_1 + a_7 a_2 \\
P_A(3) & = & a_1 a_4 + a_2 a_5 + a_3 a_6 + a_4 a_7 + a_5 a_1 + a_6 a_2 + a_7 a_3 \\
P_A(4) & = & a_1 a_4 + a_2 a_5 + a_3 a_6 + a_4 a_7 + a_5 a_1 + a_6 a_2 + a_7 a_3 \\
P_A(5) & = & a_1 a_3 + a_2 a_4 + a_3 a_5 + a_4 a_6 + a_5 a_7 + a_6 a_1 + a_7 a_2 \\
P_A(6) & = & a_1 a_2 + a_2 a_3 + a_3 a_4 + a_4 a_5 + a_5 a_6 + a_6 a_7 + a_7 a_1
\end{array}$$

Example: $n = 7$, $A = [a_1, \ldots, a_7]$

$$\begin{array}{lcl}
P_A(0) & = & a_1{}^2 + a_2{}^2 + a_3{}^2 + a_4{}^2 + a_5{}^2 + a_6{}^2 + a_7{}^2 \\
P_A(1) & = & a_1 a_2 + a_2 a_3 + a_3 a_4 + a_4 a_5 + a_5 a_6 + a_6 a_7 + a_7 a_1 \\
P_A(2) & = & a_1 a_3 + a_2 a_4 + a_3 a_5 + a_4 a_6 + a_5 a_7 + a_6 a_1 + a_7 a_2 \\
P_A(3) & = & a_1 a_4 + a_2 a_5 + a_3 a_6 + a_4 a_7 + a_5 a_1 + a_6 a_2 + a_7 a_3 \\
P_A(4) & = & a_1 a_4 + a_2 a_5 + a_3 a_6 + a_4 a_7 + a_5 a_1 + a_6 a_2 + a_7 a_3 \\
P_A(5) & = & a_1 a_3 + a_2 a_4 + a_3 a_5 + a_4 a_6 + a_5 a_7 + a_6 a_1 + a_7 a_2 \\
P_A(6) & = & a_1 a_2 + a_2 a_3 + a_3 a_4 + a_4 a_5 + a_5 a_6 + a_6 a_7 + a_7 a_1
\end{array}$$

$$\begin{array}{lcl}
N_A(0) & = & a_1{}^2 + a_2{}^2 + a_3{}^2 + a_4{}^2 + a_5{}^2 + a_6{}^2 + a_7{}^2 \\
N_A(1) & = & a_1 a_2 + a_2 a_3 + a_3 a_4 + a_4 a_5 + a_5 a_6 + a_6 a_7 \\
N_A(2) & = & a_1 a_3 + a_2 a_4 + a_3 a_5 + a_4 a_6 + a_5 a_7 \\
N_A(3) & = & a_1 a_4 + a_2 a_5 + a_3 a_6 + a_4 a_7 \\
N_A(4) & = & a_1 a_5 + a_2 a_6 + a_3 a_7 \\
N_A(5) & = & a_1 a_6 + a_2 a_7 \\
N_A(6) & = & a_1 a_7
\end{array}$$

Autoccorelation Properties

Circulant Matrices

A $n \times n$ matrix $C(A)$ is called circulant if every row (except the first) is obtained by the previous row by a right cyclic shift by one.

Circulant Matrices

A $n \times n$ matrix $C(A)$ is called circulant if every row (except the first) is obtained by the previous row by a right cyclic shift by one.

$$C(A) = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ a_2 & a_3 & \dots & a_0 & a_1 \\ a_1 & a_2 & \dots & a_{n-1} & a_0 \end{bmatrix}$$

1. Consider a finite sequence $A = [a_0, \ldots, a_{n-1}]$ of length n and the circulant matrix $C(A)$ whose first row is equal to A. Then $P_A(i)$ is the inner product of the first row of $C(A)$ and the $i+1$ row of $C(A)$.

1. Consider a finite sequence $A = [a_0, \ldots, a_{n-1}]$ of length n and the circulant matrix $C(A)$ whose first row is equal to A. Then $P_A(i)$ is the inner product of the first row of $C(A)$ and the $i+1$ row of $C(A)$.
2. **symmetry property**
   $\rightsquigarrow \quad P_A(s) = P_A(n-s), s = 1, \ldots, n-1.$

1. Consider a finite sequence $A = [a_0, \ldots, a_{n-1}]$ of length n and the circulant matrix $C(A)$ whose first row is equal to A. Then $P_A(i)$ is the inner product of the first row of $C(A)$ and the $i+1$ row of $C(A)$.
2. **symmetry property**
   $\rightsquigarrow \quad P_A(s) = P_A(n-s), s = 1, \ldots, n-1.$
3. $2^{\textbf{nd}}$ **ESF property**
   $\rightsquigarrow \quad P_A(1) + P_A(2) + \ldots + P_A(n-1) = 2e_2(a_0, \ldots, a_{n-1})$
   where $e_2(a_0, \ldots, a_{n-1})$ is the second ESF

1. Consider a finite sequence $A = [a_0, \ldots, a_{n-1}]$ of length n and the circulant matrix $C(A)$ whose first row is equal to A. Then $P_A(i)$ is the inner product of the first row of $C(A)$ and the $i+1$ row of $C(A)$.
2. **symmetry property**
   $\rightsquigarrow \quad P_A(s) = P_A(n-s), s = 1, \ldots, n-1.$
3. 2^{nd} **ESF property**
   $\rightsquigarrow \quad P_A(1) + P_A(2) + \ldots + P_A(n-1) = 2e_2(a_0, \ldots, a_{n-1})$
   where $e_2(a_0, \ldots, a_{n-1})$ is the second ESF
4. $\rightsquigarrow \quad N_A(s) + N_A(n-s) = P_A(s), s = 1, \ldots, n-1.$

Complementary Sequences

Definition

Let $\{A_i\}_{i=1,\dots,t}$ be t sequences of length v with complex elements. The sequences $\{A_i\}_{i=1,\dots,t}$ are called complementary, if

$$\sum_{i=1}^{t} PAF_{A_i} = [\alpha_0, \underbrace{\alpha, \dots, \alpha}_{v-1 \text{ terms}}]$$

with the convention:

$$PAF_{A_i} = [PAF_{A_i}(0), PAF_{A_i}(1), \dots, PAF_{A_i}(v-1)].$$

Algorithms and Metaheuristics for Combinatorial Matrices
Ilias S. Kotsireas
Handbook of Combinatorial Optimization, 2nd ed.
Pardalos, P. M., Du, D.-Z., Graham, R. L. (eds)
pp. 283-309, Springer 2013

Unified description of combinatorial objects

number/type of sequences	defining property	name
1 binary	aper. autoc. $0, \pm 1$	Barker sequences
1 ternary	per. autoc. 0	circulant weighing matrices
2 binary	aper. autoc. 0	Golay sequences
2 4-th roots	aper. autoc. 0	complex Golay sequences
2 binary	per. autoc. 0	Hadamard matrices
2 binary	per. autoc. 2	D-optimal matrices
2 binary	per. autoc. -2	Hadamard matrices
2 ternary	aper. autoc. 0	TCP
2 ternary	per. autoc. 0	Weighing matrices
3 binary	aper. autoc. const.	Normal sequences
4 binary	aper. autoc. 0	Base sequences
4 binary	aper. autoc. 0	Turyn type sequences
4 ternary	aper. autoc. 0	T-sequences
4 binary	per. autoc. 0	Williamson Hadamard
$2 \ldots 12$ binary	per. autoc. zero	PCS

Power Spectral Density, PSD

Power Spectral Density, PSD

Seberry & Gysin first introduced the PSD concept in the search for complementary sequences of various kinds.

Power Spectral Density, PSD

Seberry & Gysin first introduced the PSD concept in the search for complementary sequences of various kinds.

Definition

$PSD([a_1, \ldots, a_n], k)$ denotes the k-th element of the power spectral density sequence, i.e. the square magnitude of the k-th element of the discrete Fourier transform (DFT) sequence associated to $[a_1, \ldots, a_n]$.

Power Spectral Density, PSD

Seberry & Gysin first introduced the PSD concept in the search for complementary sequences of various kinds.

Definition

$PSD([a_1, \ldots, a_n], k)$ denotes the k-th element of the power spectral density sequence, i.e. the square magnitude of the k-th element of the discrete Fourier transform (DFT) sequence associated to $[a_1, \ldots, a_n]$.

The DFT sequence associated to $[a_1, \ldots, a_n]$ is defined as

$$DFT_{[a_1,\ldots,a_n]} = [\,\mu_0, \ldots, \mu_{n-1}\,], \text{ with } \mu_k = \sum_{i=0}^{n-1} a_{i+1}\,\omega^{ik}, \; k = 0, \ldots, n-1$$

where $\omega = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ is a primitive n-th root of unity.

PSD criterion

Williamson Hadamard matrices: 4 complementary sequences of length n, (odd)
PAF constant: 0, PSD constant: $4n$.

$$PAF(A,s)+PAF(B,s)+PAF(C,s)+PAF(D,s)=0, \quad s=1,\ldots,\frac{n-1}{2}$$

$$PSD(A,s)+PSD(B,s)+PSD(C,s)+PSD(D,s)=4n, \quad s=1,\ldots,\frac{n-1}{2}$$

if for a certain sequence $A=[a_1,\ldots,a_n]$ there exists $s\in\{1,\ldots,n-1\}$ with the property that $PSD(A,s)>4n$, then this sequence cannot be used to construct 4 such complementary sequences

Important Consequence: we can now decouple the PAF equations, roughly corresponding to cutting down the complexity by four.

Claude Monet
Haystacks, End of Summer, (Meules, fin de l'été), 1891.
Oil on canvas. Musée d'Orsay, Paris, France.

Compression of complementary sequences

Compression of complementary sequences

Definition

Let $A = [a_0, a_1, \ldots, a_{v-1}]$ be a complex sequence of length $v = dm$. Set $a_j^{(d)} = a_j + a_{j+d} + \ldots + a_{j+(m-1)d}$, for $j = 0, \ldots, d-1$. Then we say that the sequence $A^{(d)} = [a_0^{(d)}, a_1^{(d)}, \ldots, a_{d-1}^{(d)}]$ of length d is the m-compression of A.

Compression of complementary sequences

Definition

Let $A = [a_0, a_1, \ldots, a_{v-1}]$ be a complex sequence of length $v = dm$. Set $a_j^{(d)} = a_j + a_{j+d} + \ldots + a_{j+(m-1)d}$, for $j = 0, \ldots, d-1$. Then we say that the sequence $A^{(d)} = [a_0^{(d)}, a_1^{(d)}, \ldots, a_{d-1}^{(d)}]$ of length d is the m-compression of A.

PhD thesis of Yoseph Strassler, (1997), Bar-Ilan University, Israel.

Example

$A = CW(24, 9) =$
$[0, 0, 0, -1, -1, 0, 0, 0, 0, 0, 1, -1, 0, 0, 0, -1, 1, 0, 0, 1, 0, 0, -1, -1]$

Compression of complementary sequences

Definition

Let $A = [a_0, a_1, \ldots, a_{v-1}]$ be a complex sequence of length $v = dm$. Set $a_j^{(d)} = a_j + a_{j+d} + \ldots + a_{j+(m-1)d}$, for $j = 0, \ldots, d-1$. Then we say that the sequence $A^{(d)} = [a_0^{(d)}, a_1^{(d)}, \ldots, a_{d-1}^{(d)}]$ of length d is the m-compression of A.

PhD thesis of Yoseph Strassler, (1997), Bar-Ilan University, Israel.

Example

$A = CW(24, 9) =$
$[0, 0, 0, -1, -1, 0, 0, 0, 0, 0, 1, -1, 0, 0, 0, -1, 1, 0, 0, 1, 0, 0, -1, -1]$
$m = 2, \quad d = 12, \quad \rightsquigarrow \quad A^{(12)} = [0, 0, 0, -2, 0, 0, 0, 1, 0, 0, 0, -2]$

Compression of complementary sequences

Definition

Let $A = [a_0, a_1, \ldots, a_{v-1}]$ be a complex sequence of length $v = dm$. Set $a_j^{(d)} = a_j + a_{j+d} + \ldots + a_{j+(m-1)d}$, for $j = 0, \ldots, d-1$. Then we say that the sequence $A^{(d)} = [a_0^{(d)}, a_1^{(d)}, \ldots, a_{d-1}^{(d)}]$ of length d is the m-compression of A.

PhD thesis of Yoseph Strassler, (1997), Bar-Ilan University, Israel.

Example

$A = CW(24, 9) =$
$[0, 0, 0, -1, -1, 0, 0, 0, 0, 0, 1, -1, 0, 0, 0, -1, 1, 0, 0, 1, 0, 0, -1, -1]$
$m = 2, \quad d = 12, \quad \rightsquigarrow \quad A^{(12)} = [0, 0, 0, -2, 0, 0, 0, 1, 0, 0, 0, -2]$
$m = 3, \quad d = 8, \quad \rightsquigarrow \quad A^{(8)} = [1, 0, 1, -1, -1, 0, -1, -2]$

Theorem: Djokovic-Kotsireas (DCC 2012)

Theorem: Djokovic-Kotsireas (DCC 2012)

- Let $\{A_i\}_{i=1,\ldots,t}$ be t complementary sequences, of length v each, with complex elements $A_i = [a_{i0}, a_{i1}, \ldots, a_{i,v-1}]$, for $i = 1, \ldots, t$ and $\sum_{i=1}^{t} PAF_{A_i} = [\alpha_0, \underbrace{\alpha, \ldots, \alpha}_{v-1 \text{ terms}}]$.

Theorem: Djokovic-Kotsireas (DCC 2012)

- Let $\{A_i\}_{i=1,\ldots,t}$ be t complementary sequences, of length v each, with complex elements $A_i = [a_{i0}, a_{i1}, \ldots, a_{i,v-1}]$, for $i = 1, \ldots, t$ and $\sum_{i=1}^{t} PAF_{A_i} = [\alpha_0, \underbrace{\alpha, \ldots, \alpha}_{v-1 \text{ terms}}]$.
- Assume that $v = dm$ and set $a_{ij}^{(d)} = a_{i,j} + a_{i,j+d} + \cdots + a_{i,j+(m-1)d}, i = 1, \ldots, t, j = 0, \ldots, d-1.$

Theorem: Djokovic-Kotsireas (DCC 2012)

- Let $\{A_i\}_{i=1,\ldots,t}$ be t complementary sequences, of length v each, with complex elements $A_i = [a_{i0}, a_{i1}, \ldots, a_{i,v-1}]$, for $i = 1, \ldots, t$ and $\sum_{i=1}^{t} PAF_{A_i} = [\alpha_0, \underbrace{\alpha, \ldots, \alpha}_{v-1 \text{ terms}}]$.
- Assume that $v = dm$ and set $a_{ij}^{(d)} = a_{i,j} + a_{i,j+d} + \cdots + a_{i,j+(m-1)d}, i = 1, \ldots, t, j = 0, \ldots, d-1.$
- Then the t m-compressed sequences $\{A_i^{(d)}\}_{i=1,\ldots,t}$, of length d each, are also complementary

Theorem: Djokovic-Kotsireas (DCC 2012)

- Let $\{A_i\}_{i=1,\ldots,t}$ be t complementary sequences, of length v each, with complex elements $A_i = [a_{i0}, a_{i1}, \ldots, a_{i,v-1}]$, for $i = 1, \ldots, t$ and $\sum_{i=1}^{t} PAF_{A_i} = [\alpha_0, \underbrace{\alpha, \ldots, \alpha}_{v-1 \text{ terms}}]$.
- Assume that $v = dm$ and set $a_{ij}^{(d)} = a_{i,j} + a_{i,j+d} + \cdots + a_{i,j+(m-1)d}, i = 1, \ldots, t, j = 0, \ldots, d-1$.
- Then the t m-compressed sequences $\{A_i^{(d)}\}_{i=1,\ldots,t}$, of length d each, are also complementary

$$\sum_{i=1}^{t} PAF_{A_i^{(d)}} = [\alpha_0 + (m-1)\alpha, \underbrace{m\alpha, \ldots, m\alpha}_{d-1 \text{ terms}}]$$

Theorem: Djokovic-Kotsireas (DCC 2012)

- Let $\{A_i\}_{i=1,\ldots,t}$ be t complementary sequences, of length v each, with complex elements $A_i = [a_{i0}, a_{i1}, \ldots, a_{i,v-1}]$, for $i = 1, \ldots, t$ and $\sum_{i=1}^{t} PAF_{A_i} = [\alpha_0, \underbrace{\alpha, \ldots, \alpha}_{v-1 \text{ terms}}]$.
- Assume that $v = dm$ and set $a_{ij}^{(d)} = a_{i,j} + a_{i,j+d} + \cdots + a_{i,j+(m-1)d}, i = 1, \ldots, t, j = 0, \ldots, d-1.$
- Then the t m-compressed sequences $\{A_i^{(d)}\}_{i=1,\ldots,t}$, of length d each, are also complementary

$$\sum_{i=1}^{t} PAF_{A_i^{(d)}} = [\alpha_0 + (m-1)\alpha, \underbrace{m\alpha, \ldots, m\alpha}_{d-1 \text{ terms}}]$$

$$\sum_{i=1}^{t} PSD_{A_i^{(d)}} = [\beta_0, \underbrace{\beta, \ldots, \beta}_{d-1 \text{ terms}}]$$

Periodic Golay pairs of length 68

Consider the following two sequences of length 34 each, with $\{-2, 0, +2\}$ elements:

$$A^{(34)} = [0, 0, 0, 2, 0, 0, -2, 0, 0, 0, 2, -2, 0, 0, -2, 0, 0, 2, 0, 0, 0, 2, 2, -2, 0, 0, -2, 0, 0, 2, 0, 2, 0, 2]$$
$$B^{(34)} = [0, 0, -2, 2, 0, 2, 0, -2, -2, 0, 2, 2, 0, 2, -2, 0, 2, 0, -2, 2, 0, 2, 2, 0, 2, 0, 2, 2, 0, -2, 2, 0, -2, -2]$$

These two sequences satisfy the following properties:

1. $\mathrm{PAF}(A^{(34)}, s) + \mathrm{PAF}(B^{(34)}, s) = 0, s = 1, \ldots, 33;$
2. $\mathrm{PSD}(A^{(34)}, s) + \mathrm{PSD}(B^{(34)}, s) = 2 \cdot 68 = 136, s = 1, \ldots, 33;$
3. $\mathrm{PSD}(A^{(34)}, 17) = 100$ and $\mathrm{PSD}(B^{(34)}, 17) = 36;$
4. $\sum_{i=1}^{34} A_i^{(34)} = 6$ and $\sum_{i=1}^{34} B_i^{(34)} = 10; \quad 6^2 + 10^2 = 2 \cdot 68$
5. The total number of 0 elements in $A^{(34)}$ and $B^{(34)}$ is 34;
6. The total number of ± 2 elements in $A^{(34)}$ and $B^{(34)}$ is 34;
7. $A^{(34)}$ contains 21 zeros and $B^{(34)}$ contains 13 zeros.

Periodic Golay pairs of length 68

$A^{(34)}$ and $B^{(34)}$ are the 2-compressed sequences of two $\{-1,+1\}$ sequences of length 68 each, that form a particular **periodic Golay pair of length** 68:

$$
\begin{array}{ccl}
A & = & --++-+-+-++--+--++---++------+-+++ \\
  &   & ++-++---+-+-+--+-++++++-++-+++++-+ \\
B & = & ---+++---+++++--++-+-+++++++--+--- \\
  &   & ++-+-++---++-+-++--++++-+-+++-++--
\end{array}
$$

$\rightsquigarrow$ Hadamard matrices of order $2 \cdot 68$

Reference

Djokovic, Dragomir; Kotsireas, Ilias; Recoskie, Daniel; Sawada, Joe
Charm bracelets and their application to the construction of periodic Golay pairs. Discrete Appl. Math. 188 (2015), 32-40.

The new petaflop Canadian HPC landscape

The new petaflop Canadian HPC landscape

June 2018 `top500.org` list is out!

The new petaflop Canadian HPC landscape

June 2018 `top500.org` list is out!

- No 53, University of Toronto, Niagara, 60K cores

The new petaflop Canadian HPC landscape

June 2018 `top500.org` list is out!

- No 53, University of Toronto, Niagara, 60K cores
- No 147, Simon Fraser University, Cedar, 59,776 cores

The new petaflop Canadian HPC landscape

June 2018 top500.org list is out!

- No 53, University of Toronto, Niagara, 60K cores
- No 147, Simon Fraser University, Cedar, 59,776 cores
- No 166, University of Waterloo, Graham, 51,200 cores

https://docs.computecanada.ca/wiki/Graham

2015 http://top500.org/

2015 http://top500.org/

TIANHE-2	(MILKYWAY-2)
Site:	National Super Computer Center, Guangzhou
Cores:	3,120,000
Linpack Perf (Rmax)	33,862.7 TFlop/s
Theoretical Peak (Rpeak)	54,902.4 TFlop/s
Memory:	1,024,000 GB
Processor:	Intel Xeon E5-2692v2 12C 2.2GHz
Compiler:	icc

2015 http://top500.org/

TIANHE-2	(MILKYWAY-2)
Site:	National Super Computer Center, Guangzhou
Cores:	3,120,000
Linpack Perf (Rmax)	33,862.7 TFlop/s
Theoretical Peak (Rpeak)	54,902.4 TFlop/s
Memory:	1,024,000 GB
Processor:	Intel Xeon E5-2692v2 12C 2.2GHz
Compiler:	icc

2007: open problem, 2^{50} ops $\rightsquigarrow$ 2015: ex. search in 10 minutes

SAT encodings of Autocorrelation

SAT encodings of Autocorrelation

D-optimal designs

S. Arunachalam, I. Kotsireas
Hard satisfiable 3-SAT instances via autocorrelation.
J. Satisf. Boolean Model. Comput. 10 (2016), pp. 11–22.

SAT encodings of Autocorrelation

D-optimal designs

S. Arunachalam, I. Kotsireas
Hard satisfiable 3-SAT instances via autocorrelation.
J. Satisf. Boolean Model. Comput. 10 (2016), pp. 11–22.

1. Two $\{\pm 1\}$ sequences of odd length n, with PAF constant 2 and PSD constant $2n-2$, Diophantine Equation $a^2 + b^2 = 4n - 2$.

SAT encodings of Autocorrelation

D-optimal designs

S. Arunachalam, I. Kotsireas
Hard satisfiable 3-SAT instances via autocorrelation.
J. Satisf. Boolean Model. Comput. 10 (2016), pp. 11–22.

1. Two $\{\pm 1\}$ sequences of odd length n, with PAF constant 2 and PSD constant $2n-2$, Diophantine Equation $a^2+b^2=4n-2$.
2. Tools: CSP, Tseitin transformation, comparators, half-adders, full-adders, Matlab generator of 3-SAT instances

SAT encodings of Autocorrelation

D-optimal designs

S. Arunachalam, I. Kotsireas
Hard satisfiable 3-SAT instances via autocorrelation.
J. Satisf. Boolean Model. Comput. 10 (2016), pp. 11–22.

1. Two $\{\pm 1\}$ sequences of odd length n, with PAF constant 2 and PSD constant $2n-2$, Diophantine Equation $a^2+b^2=4n-2$.
2. Tools: CSP, Tseitin transformation, comparators, half-adders, full-adders, Matlab generator of 3-SAT instances

SC 2014 Vienna

Proceedings of SAT COMPETITION 2014
Solver and Benchmark Descriptions
Anton Belov, Daniel Diepold, Marijn J.H. Heule, and Matti Järvisalo (editors)

SAT encodings of Autocorrelation

Motivational Quote

"From 100 variables, 200 clauses (early 90s) to 1,000,000 variables and 5,000,000 clauses in 15 years". In: Marijn J.H. Heule, Warren A. Hunt Jr. Practical SAT Solving Course Notes, The University of Texas at Austin, 2013

SAT encodings of Autocorrelation

Motivational Quote

"From 100 variables, 200 clauses (early 90s) to 1,000,000 variables and 5,000,000 clauses in 15 years". In: Marijn J.H. Heule, Warren A. Hunt Jr. Practical SAT Solving Course Notes, The University of Texas at Austin, 2013

Williamson Hadamard matrices

Curtis Bright
Computational Methods for Combinatorial and Number Theoretic Problems
PhD Thesis, 2017, University of Waterloo

Example: Williamson Sequences of Order 3

Example: Williamson Sequences of Order 3

Objective:

Example: Williamson Sequences of Order 3

Objective:

- Find ± 1 values for vars a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 which satisfy the constraint $a_0 a_1 + b_0 b_1 + c_0 c_1 + d_0 d_1 + 2 = 0$

Example: Williamson Sequences of Order 3

Objective:

- Find ± 1 values for vars a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 which satisfy the constraint $a_0 a_1 + b_0 b_1 + c_0 c_1 + d_0 d_1 + 2 = 0$

Linearization:

Example: Williamson Sequences of Order 3

Objective:

- Find ± 1 values for vars a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 which satisfy the constraint $a_0 a_1 + b_0 b_1 + c_0 c_1 + d_0 d_1 + 2 = 0$

Linearization:

- Let $p_0 := a_0 a_1$, $p_1 := b_0 b_1$, $p_2 := c_0 c_1$, $p_3 := d_0 d_1$

Example: Williamson Sequences of Order 3

Objective:

- Find ± 1 values for vars a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 which satisfy the constraint $a_0 a_1 + b_0 b_1 + c_0 c_1 + d_0 d_1 + 2 = 0$

Linearization:

- Let $p_0 := a_0 a_1$, $p_1 := b_0 b_1$, $p_2 := c_0 c_1$, $p_3 := d_0 d_1$
- The constraint now becomes $p_0 + p_1 + p_2 + p_3 + 2 = 0$

Example: Williamson Sequences of Order 3

Objective:

- Find ± 1 values for vars a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 which satisfy the constraint $a_0 a_1 + b_0 b_1 + c_0 c_1 + d_0 d_1 + 2 = 0$

Linearization:

- Let $p_0 := a_0 a_1$, $p_1 := b_0 b_1$, $p_2 := c_0 c_1$, $p_3 := d_0 d_1$
- The constraint now becomes $p_0 + p_1 + p_2 + p_3 + 2 = 0$

Rewrite as a Cardinality Constraint:

Example: Williamson Sequences of Order 3

Objective:

- Find ± 1 values for vars a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 which satisfy the constraint $a_0 a_1 + b_0 b_1 + c_0 c_1 + d_0 d_1 + 2 = 0$

Linearization:

- Let $p_0 := a_0 a_1$, $p_1 := b_0 b_1$, $p_2 := c_0 c_1$, $p_3 := d_0 d_1$
- The constraint now becomes $p_0 + p_1 + p_2 + p_3 + 2 = 0$

Rewrite as a Cardinality Constraint:

- Since $p_0 + p_1 + p_2 + p_3 + 2 = 0$ and each $p_i \in \{\pm 1\}$, we determine that $\#\{\, i : p_i = 1 \,\} = 1$ and $\#\{\, i : p_i = -1 \,\} = 3$

Example: Williamson Sequences of Order 3

Objective:

- Find ± 1 values for vars a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 which satisfy the constraint $a_0 a_1 + b_0 b_1 + c_0 c_1 + d_0 d_1 + 2 = 0$

Linearization:

- Let $p_0 := a_0 a_1$, $p_1 := b_0 b_1$, $p_2 := c_0 c_1$, $p_3 := d_0 d_1$
- The constraint now becomes $p_0 + p_1 + p_2 + p_3 + 2 = 0$

Rewrite as a Cardinality Constraint:

- Since $p_0 + p_1 + p_2 + p_3 + 2 = 0$ and each $p_i \in \{\pm 1\}$, we determine that $\#\{\, i : p_i = 1 \,\} = 1$ and $\#\{\, i : p_i = -1 \,\} = 3$

Determining a Conflict Clause:

Example: Williamson Sequences of Order 3

Objective:

- Find ± 1 values for vars a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 which satisfy the constraint $a_0 a_1 + b_0 b_1 + c_0 c_1 + d_0 d_1 + 2 = 0$

Linearization:

- Let $p_0 := a_0 a_1$, $p_1 := b_0 b_1$, $p_2 := c_0 c_1$, $p_3 := d_0 d_1$
- The constraint now becomes $p_0 + p_1 + p_2 + p_3 + 2 = 0$

Rewrite as a Cardinality Constraint:

- Since $p_0 + p_1 + p_2 + p_3 + 2 = 0$ and each $p_i \in \{\pm 1\}$, we determine that $\#\{\, i : p_i = 1 \,\} = 1$ and $\#\{\, i : p_i = -1 \,\} = 3$

Determining a Conflict Clause:

- Say the SAT solver finds a partial assignment with $\{p_0 = 1, p_1 = -1, p_2 = 1\}$

Example: Williamson Sequences of Order 3

Objective:

- Find ± 1 values for vars a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 which satisfy the constraint $a_0 a_1 + b_0 b_1 + c_0 c_1 + d_0 d_1 + 2 = 0$

Linearization:

- Let $p_0 := a_0 a_1$, $p_1 := b_0 b_1$, $p_2 := c_0 c_1$, $p_3 := d_0 d_1$
- The constraint now becomes $p_0 + p_1 + p_2 + p_3 + 2 = 0$

Rewrite as a Cardinality Constraint:

- Since $p_0 + p_1 + p_2 + p_3 + 2 = 0$ and each $p_i \in \{\pm 1\}$, we determine that $\#\{\, i : p_i = 1 \,\} = 1$ and $\#\{\, i : p_i = -1 \,\} = 3$

Determining a Conflict Clause:

- Say the SAT solver finds a partial assignment with $\{p_0 = 1, p_1 = -1, p_2 = 1\}$
- Since $\#\{\, i : p_i = 1 \,\} > 1$, we know that this assignment can never result in an actual solution to the problem.

Example: Williamson Sequences of Order 3

Objective:

- Find ± 1 values for vars $a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1$ which satisfy the constraint $a_0 a_1 + b_0 b_1 + c_0 c_1 + d_0 d_1 + 2 = 0$

Linearization:

- Let $p_0 := a_0 a_1$, $p_1 := b_0 b_1$, $p_2 := c_0 c_1$, $p_3 := d_0 d_1$
- The constraint now becomes $p_0 + p_1 + p_2 + p_3 + 2 = 0$

Rewrite as a Cardinality Constraint:

- Since $p_0 + p_1 + p_2 + p_3 + 2 = 0$ and each $p_i \in \{\pm 1\}$, we determine that $\#\{\, i : p_i = 1 \,\} = 1$ and $\#\{\, i : p_i = -1 \,\} = 3$

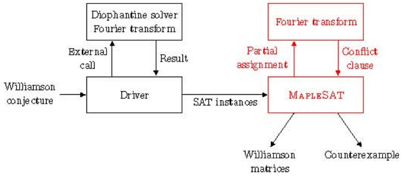
Determining a Conflict Clause:

- Say the SAT solver finds a partial assignment with $\{p_0 = 1, p_1 = -1, p_2 = 1\}$
- Since $\#\{\, i : p_i = 1 \,\} > 1$, we know that this assignment can never result in an actual solution to the problem.
- We tell the SAT solver to learn the constraint

$$\neg(\{p_0 = 1\} \wedge \{p_2 = 1\})$$

Solution: Programmatic SAT

- A *programmatic* SAT solver[5] contains a special *callback* function which periodically examines the current partial assignment while the SAT solver is running.
- If it can determine that the partial assignment cannot be extended into a satisfying assignment then a conflict clause is generated encoding that fact.

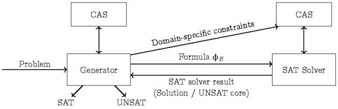


[5] V. Ganesh et al., LYNX: A programmatic SAT solver for the RNA-folding problem, SAT 2012.

MathCheck

https://sites.google.com/site/uwmathcheck

The MATHCHECK2 System



MathCheck main reference

Zulkoski, Edward; Bright, Curtis; Heinle, Albert; Kotsireas, Ilias; Czarnecki, Krzysztof; Ganesh, Vijay
Combining SAT solvers with computer algebra systems to verify combinatorial conjectures
J. Automat. Reason. 58 (2017), no. 3, pp. 313–339

Conjectures studied by MathCheck

Conjectures studied by MathCheck

1. Ruskey-Savage conjecture (1993): Any matching of a hypercube can be extended to a Hamiltonian cycle. MathCheck: Conjecture holds for hypercubes of dimension $d \leq 5$.

Conjectures studied by MathCheck

1. Ruskey-Savage conjecture (1993): Any matching of a hypercube can be extended to a Hamiltonian cycle.
   MathCheck: Conjecture holds for hypercubes of dimension $d \leq 5$.
2. Norine conjecture (2008): There always exists a monochromatic path between two antipodal vertices in an edge-antipodal coloring of a hypercube.
   MathCheck: Conjecture holds for hypercubes of dimension $d \leq 6$.

Conjectures studied by MathCheck

1. Ruskey-Savage conjecture (1993): Any matching of a hypercube can be extended to a Hamiltonian cycle.
   MathCheck: Conjecture holds for hypercubes of dimension $d \leq 5$.
2. Norine conjecture (2008): There always exists a monochromatic path between two antipodal vertices in an edge-antipodal coloring of a hypercube.
   MathCheck: Conjecture holds for hypercubes of dimension $d \leq 6$.
3. Hadamard conjecture (1893): Hadamard matrices exist for all orders divisible by 4.
   MathCheck: Williamson-generated Hadamard matrices exist for all orders 4n with $n < 35$ but not for $n = 35$. They exist for $n = 63$ (open problem)

Conjectures studied by MathCheck

1. Ruskey-Savage conjecture (1993): Any matching of a hypercube can be extended to a Hamiltonian cycle.
   MathCheck: Conjecture holds for hypercubes of dimension $d \leq 5$.
2. Norine conjecture (2008): There always exists a monochromatic path between two antipodal vertices in an edge-antipodal coloring of a hypercube.
   MathCheck: Conjecture holds for hypercubes of dimension $d \leq 6$.
3. Hadamard conjecture (1893): Hadamard matrices exist for all orders divisible by 4.
   MathCheck: Williamson-generated Hadamard matrices exist for all orders 4n with $n < 35$ but not for $n = 35$. They exist for $n = 63$ (open problem)
4. Complex Golay conjecture (2002): Complex Golay sequences do not exist for order 23.
   MathCheck: Confirmation of the conjecture

Other significant Hard Combinatorial Problems

- Marijn J. H. Heule (2018). Schur Number Five. Proceedings of AAAI-18, pp. 6598–6606.
- Marijn J. H. Heule (2018). Computing Small Unit-Distance Graphs with Chromatic Number 5. To appear in Geombinatorics XXVIII(1)
- Marijn J. H. Heule, Oliver Kullmann, and Armin Biere (2018). Cube and Conquer for Satisfiability. Handbook of Parallel Constraint Reasoning, Chapter 2, pp. 31-59.
- Marijn J. H. Heule (2017). Avoiding Triples in Arithmetic Progression. Journal of Combinatorics 8(3): 391–422

On-going and future work

On-going and future work

- expand the reach of MathCheck to other autocorrelation-based combinatorial problems

On-going and future work

- expand the reach of MathCheck to other autocorrelation-based combinatorial problems
- improve the quality of the encodings

On-going and future work

- expand the reach of MathCheck to other autocorrelation-based combinatorial problems
- improve the quality of the encodings
- incorporate more effectively the consequences of PSD filtering and compression

On-going and future work

- expand the reach of MathCheck to other autocorrelation-based combinatorial problems
- improve the quality of the encodings
- incorporate more effectively the consequences of PSD filtering and compression
- apply the Cube and Conquer methodology to autocorrelation-based combinatorial problems

On-going and future work

- expand the reach of MathCheck to other autocorrelation-based combinatorial problems
- improve the quality of the encodings
- incorporate more effectively the consequences of PSD filtering and compression
- apply the Cube and Conquer methodology to autocorrelation-based combinatorial problems
- improve our understanding of the application of Programmatic SAT to autocorrelation-based combinatorial problems

On-going and future work

- expand the reach of MathCheck to other autocorrelation-based combinatorial problems
- improve the quality of the encodings
- incorporate more effectively the consequences of PSD filtering and compression
- apply the Cube and Conquer methodology to autocorrelation-based combinatorial problems
- improve our understanding of the application of Programmatic SAT to autocorrelation-based combinatorial problems

> Is this now the limit of what we can do? It may very well be, but certainly advances will not be made by people who think they cannot succeed.
>
> Carl Pomerance