Hadamard-Walsh-Fourier Transform: History and applications

Presented by Zhiwei Zhang

May 20, 2020

Fourier Transform

Boolean formulas → Multilinear Polynomials

$f : \{1, -1\}^n \to \{1, -1\}$

{F, T}

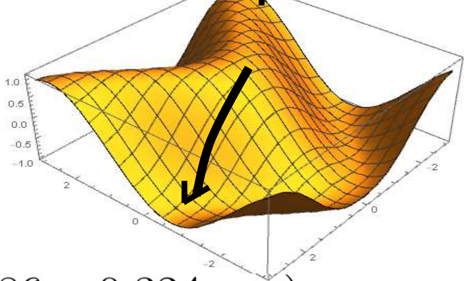
$p : \{1, -1\}^n \to \{1, -1\}$

$$x \wedge y \rightarrow \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot x + \frac{1}{2} \cdot y - \frac{1}{2} \cdot xy$$

$$\begin{aligned} f &= (x_1 \vee \neg x_2) \\ &\wedge (x_2 \oplus x_3 \oplus x_4) \\ &\wedge (x_4 + x_5 + x_6 + x_9 \geq 2) \\ &\ldots \end{aligned}$$

hybrid Boolean formula

continuous optimization



$(0.586, -0.324, \cdots)$

[1] (FourierSAT)

Fourier Transform [2,3]

spectrum coefficients

$$\boxed{\frac{1}{2}} \cdot 1 + \boxed{\frac{1}{2}} \cdot x_1 + \boxed{\frac{1}{2}} \cdot x_2 \boxed{- \frac{1}{2}} \cdot x_1 x_2$$

Orthonormal Basis functions

$$\hat{f}(S) = \sum_{x \in \{-1,1\}^n} f(x) \cdot \prod_{i \in S} x_i$$

$x \wedge y$

x_1	x_2	f
1	1	1
1	−1	1
−1	1	1
−1	−1	−1

coefficients measure how close f is to basis functions

(On how many inputs f agrees with a basis function)

computing $\hat{f}(\emptyset)$ is equivalent to model counting

$$\hat{f}(\emptyset) = \frac{1}{4}(f(0) + f(1) + f(2) + f(3)) = \frac{1}{2}$$

$$\hat{f}(\{1\}) = \frac{1}{4}(f(0) - f(1) + f(2) - f(3)) = \frac{1}{2}$$

$$\hat{f}(\{2\}) = \frac{1}{4}(f(0) + f(1) - f(2) - f(3)) = \frac{1}{2}$$

$$\hat{f}(\{1,2\}) = \frac{1}{4}(f(0) - f(1) - f(2) + f(3)) = -\frac{1}{2}$$

Hadamard Matrix $H_2(\{1,-1\}^{2^n \times 2^n})$

$$\begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \\ -1/2 \end{pmatrix} = \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}$$

Fourier Coefficients/spectrum

value

Walsh-Hadamard Transform [4,5]

Hadamard Matrix $H_2(\{1,-1\}^{2^n \times 2^n})$

$$\begin{pmatrix} \boxed{\begin{matrix} 1/2 \\ 1/2 \\ 1/2 \\ -1/2 \end{matrix}} \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} \boxed{\begin{matrix} 1 \\ 1 \\ 1 \\ -1 \end{matrix}} \end{pmatrix}$$

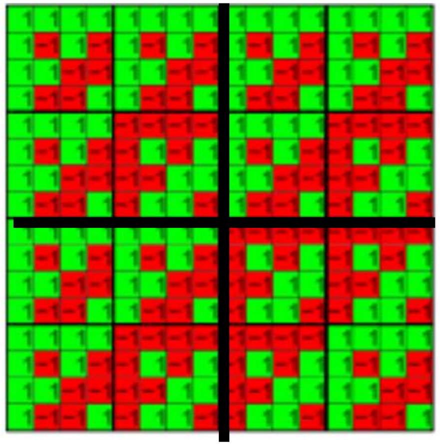
Fourier Coefficients/spectrum

value

$$H_0 = 1$$
$$H_m = \frac{1}{\sqrt{2}}\begin{pmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{pmatrix}$$

symmetric

involutive $H_n = \frac{n}{2^n} H_n^{-1}$



$$\mathbf{A}^0 = [\ 1\ ] \quad \mathbf{A}^n = \begin{bmatrix} \mathbf{A}^{n-1} & 0 \\ -\mathbf{A}^{n-1} & \mathbf{A}^{n-1} \end{bmatrix}$$

Arithmetic transform

$$\mathbf{M}^0 = [\ 1\ ] \quad \mathbf{M}^n = \begin{bmatrix} \mathbf{M}^{n-1} & 0 \\ \mathbf{M}^{n-1} & \mathbf{M}^{n-1} \end{bmatrix}$$

Reed-Muller Transform

Complexity of Hadamard-Walsh Transform: $O(2^n \cdot 2^n)$

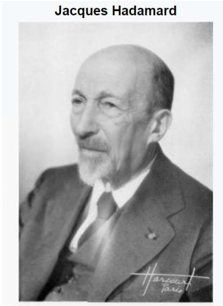
History

Jacques Hadamard

1865-1963

Hadamard Matrix (1893)

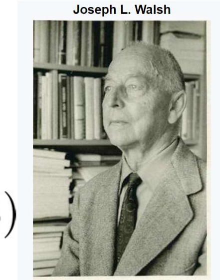
error correcting code



Joseph L. Walsh

1895-1973

orthonormal basis functions (1923)



Walsh-Hadamard Transform

Computational Engineering

"A transfrom from vector to vector"

1930s

Efficient Transform Implementation

Boolean function Classifications

Boolean Synthesis

Signal compression

Boolean Testing [11]

Fourier Analysis on Boolean Functions

Theoretical Computer science

"Harmonic Analysis"

1960s

milestones:
- Hypercontractivity (1970) [3]
- KKL Theorem (1988) [3]

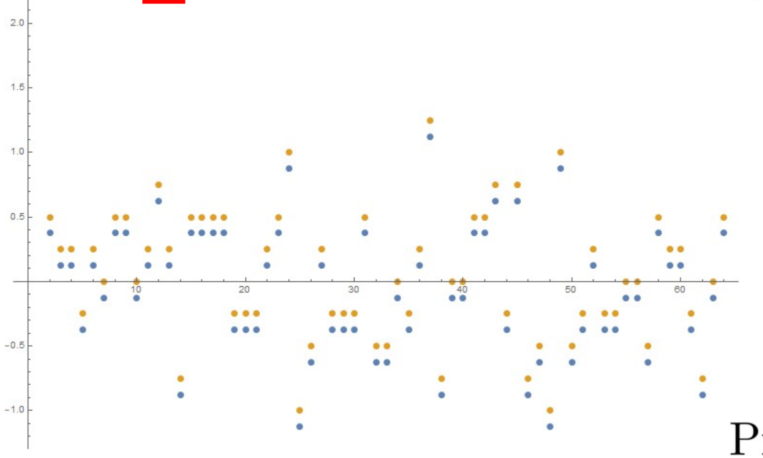
applications in theory:
- Phase transition [7]
- circuit complexity [6]
- Hardness of Approximation [21]

application in theory:
- Partition Function [8]
- Hash function [9]

Applications due to Global Information and Concentration

$$a = \{\boxed{0}, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1\}$$

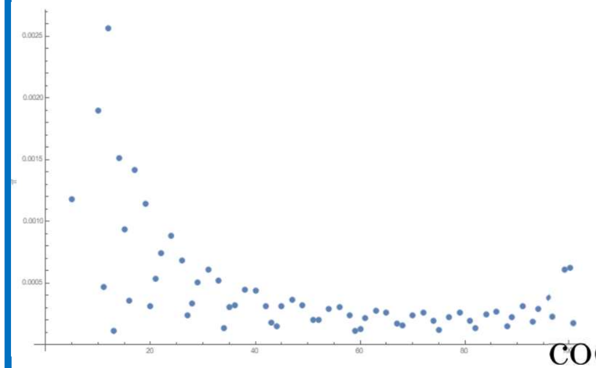
$$b = \{\boxed{1}, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1\}$$



(some) spectrum coefficients provides a spectrum signature of a Boolean function [11]

No need to compute all spectrum coefficients

Property 1: Every coefficient containts global information



learn/approximate Boolean fucntions [18]

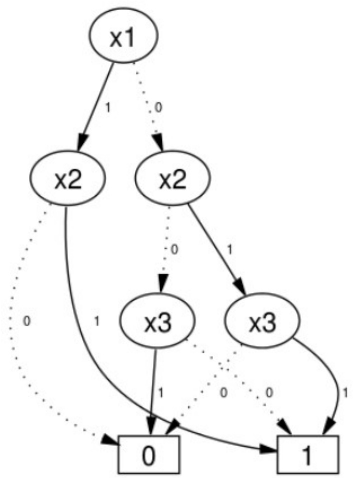
Hadamard Transform only requires plus and minus

Data compressing (JPEG)

Property 2: The spectrum "weight" often concentrates on a small set of coefficients

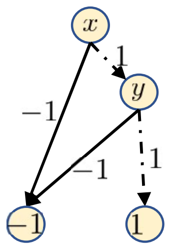
Applications: Boolean Synthesis

x1	x2	x3	*f*
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1



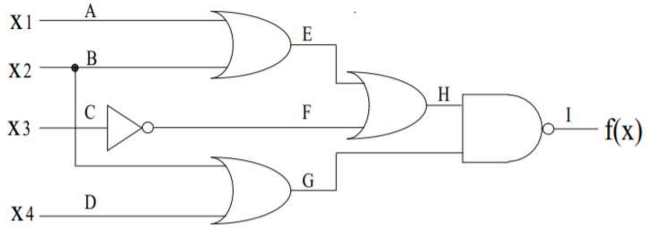
[13] (BDD)

specification



Binary decision diagram(BDD)

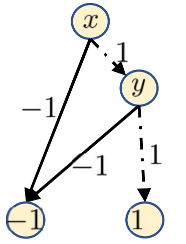
implementation



Boolean circuit

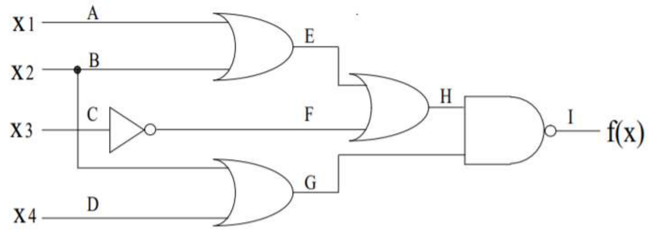
Applications: Boolean Synthesis [12]

specification

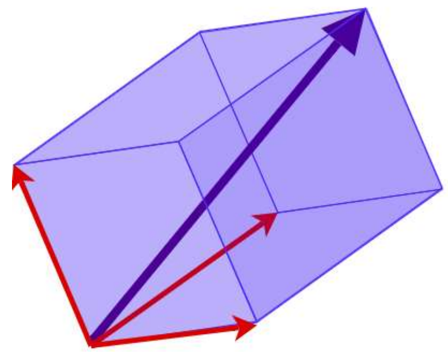


Binary decision diagram(BDD)

implementation



Boolean circuit

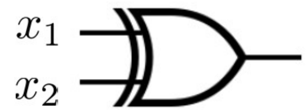


$f_e = f$

$c =$ constant circuit

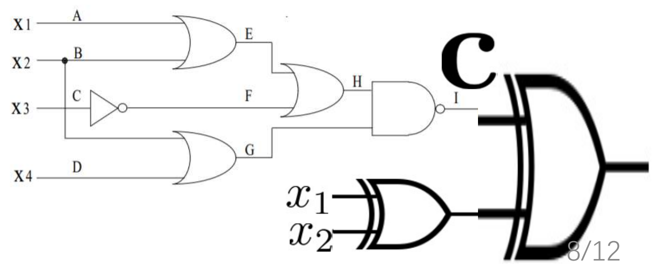
$[4, \boxed{9}, -1, 0, \cdots, 2]$

compute the Spectrum of f_e



$f_b = x_1 \oplus x_2$

find the largest coefficient
and its corresponding basis function



$f_e = f_e \oplus f_b$

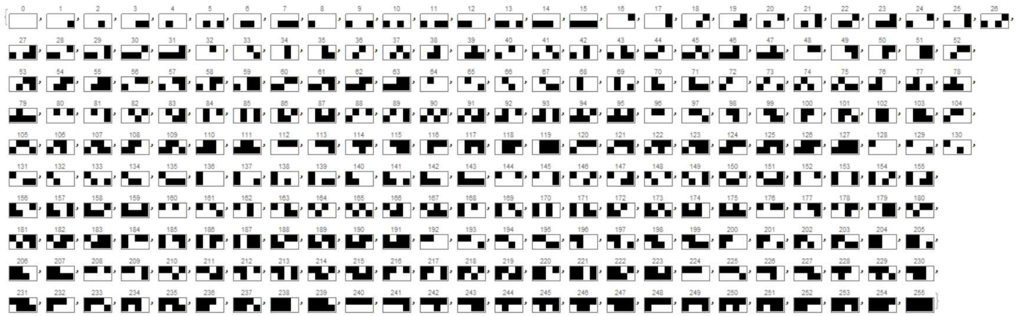
$|f_e| < \epsilon?$

N

Applications: Boolean classification [10]

Given n variables, there are 2^{2^n} different Boolean functions.

$n = 3:$



n=5,
2^{2^5}=4,294,967,296 functions

negation of output

$$g = \neg f(x_1, x_2, x_3)$$

negation of variables

$$g = f(x_1, \neg x_2, x_3)$$

permutation of variables

$$g = f(x_2, x_3, x_1)$$

variable replacement with XOR

$$g = f(x_1 \oplus x_2, x_2, x_3)$$

output replacement with XOR

$$g \oplus x_3 = f(x_1, x_2, x_3)$$

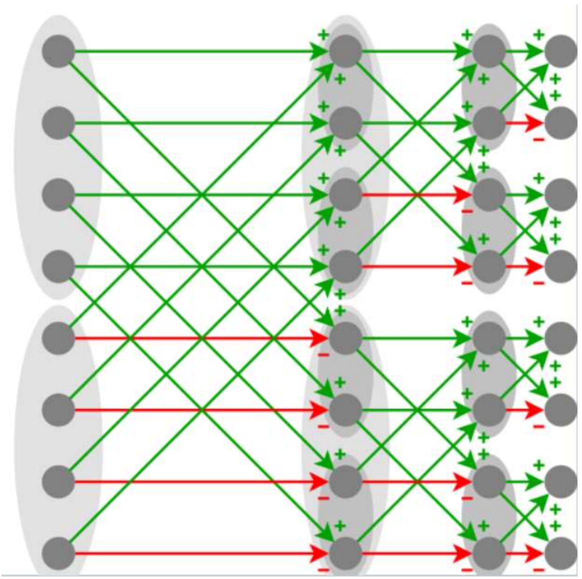
206 equivalent classes

Solve the problem in spectrum domain

Fast Hadamard Transform [14]

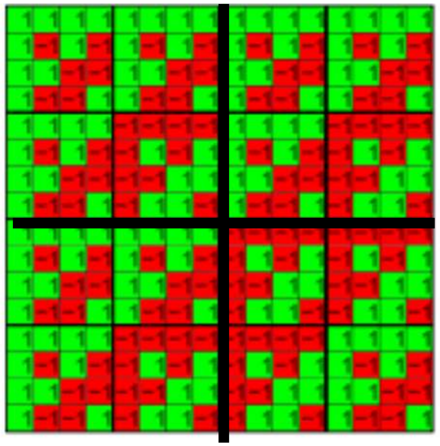
$$H_0 = 1$$
$$H_m = \frac{1}{\sqrt{2}}\begin{pmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{pmatrix}$$

values coefficients



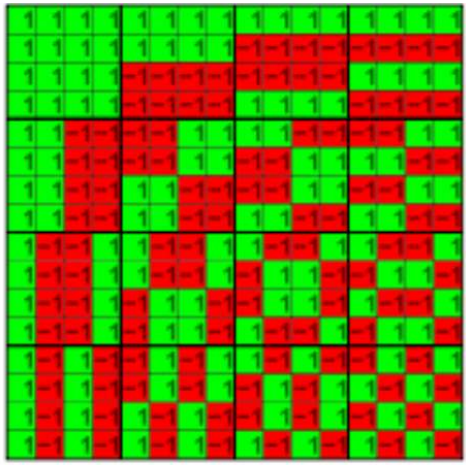
butterfly circuit

Divide and Conquer



Hadamard Matrix

rearrange



Walsh Matrix

$$\text{Complexity: } O(n \cdot 2^n)$$

$$\cancel{\text{Complexity: } O(2^n 2^n)}$$

BDD based Approach [15,16,20]

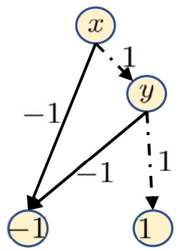
Hadamard Matrix $H_2(\{1,-1\}^{2^n \cdot 2^n})$

$$\frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} \hat{f}(\emptyset) \\ \hat{f}(\{1\}) \\ \hat{f}(\{2\}) \\ \hat{f}(\{1,2\}) \end{pmatrix}$$

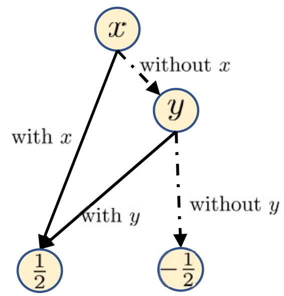
value

Fourier Coefficients

DD operations



Binary decision diagram(BDD)



Spectral Desision Diagram (SDD)

BDD with size S $\xrightarrow{O(S^2)}$ SDD with size $O(S)$

Hadamard-Walsh Transform is efficient on Boolean functions with succinct binary decision diagrams.

Summary

1. Walsh-Hadamard-Fourier Transform has many applications in theory and practice

2. History: The study of the transform splits into two directions with limited connection with each other

3. The transform can be related with lots of concepts in Boolean logic, such as BDD, model counting, synthesis...

References

[1] A. Kyrillidis, A. Shrivastava, M. Y. Vardi, Z. Zhang, FourierSAT: A Fourier 915 Expansion-Based Algebraic Framework for Solving Hybrid Boolean Constraints, in: AAAI, 2020. (FourierSAT)

[2] https://en.wikipedia.org/wiki/Hadamard_transform

[3] R. ODonnell, Analysis of Boolean Functions, Cambridge University Press, New York, NY, USA, 2014. (a very nice and complete textbook)

[4] https://en.wikipedia.org/wiki/Hadamard_matrix

[5] Thornton, M. A., D. M. Miller, and R. Drechsler, "Transformations amongst the Walsh, Haar, arithmetic and Reed-Muller spectral domains," (different transforms)

[6] A. Tal, Tight bounds on the fourier spectrum of ac0, in: Proceedings of the 930 32nd Computational Complexity Conference, CCC 17, Schloss Dagstuhl Leibniz-Zentrum fuer Informatik, Dagstuhl, DEU, 2017. (circuit complexity)

[7] G. Kalai, S. Safra, Threshold phenomena and influence, with some perspectives from mathematics, computer science, and economics, Discussion paper series, The Federmann Center for the Study of Rationality, the He935 brew University, Jerusalem (2005). (phase transition)

References

[8] Y. Xue, S. Ermon, R. Le Bras, C. P. Gomes, B. Selman, Variable Elimination in the Fourier Domain, arXiv e-prints (2015) arXiv:1508.04032arXiv: 1508.04032 (partition function)

[9] T. Achim, A. Sabharwal, S. Ermon, Beyond Parity Constraints: Fourier Analysis of Hash Functions for Inference, in: ICML, 2016, pp. 22542262. URL http://proceedings.mlr.press/v48/achim16.html (hash function)

[10] N. Anderson, The classification of Boolean functions using the Rademacher-Walsh transform, M.S. thesis, University of Victoria, 2007. (classification)

[11] J. Moore, K. Fazel, M. A. Thornton, D. M. Miller, Boolean function matching using walsh spectral decision diagrams, in: 2006 IEEE Dallas/CAS Workshop on Design, Applications, Integration and Software, 2006, pp. 127130 (Boolean matching)

[12] M. A. Thornton, V. S. S. Nair, Efficient calculation of spectral coefficients and their applications, IEEE Transactions on Computer-Aided Design of 955 Integrated Circuits and Systems 14 (11) (1995) 13281341 (Synthesis)

[13] https://en.wikipedia.org/wiki/Binary_decision_diagram (BDD)

[14] https://en.wikipedia.org/wiki/Fast_Walsh-Hadamard_transform

[15] J. Moore, K. Fazel, M. A. Thornton, D. M. Miller, Boolean function match-ing using walsh spectral decision diagrams, in: 2006 IEEE Dallas/CAS960Workshop on Design, Applications, Integration and Software, 2006, pp.127130. (BDD to SDD)

[16] M. Thornton, R. Drechsler, D. Miller, Spectral techniques in vlsi caddoi:10.1007/978-1-4615-1425-1. (BDD to SDD)

[17] Ronald de Wolf (2008). A Brief Introduction to Fourier Analysis on the Boolean Cube. Theory of Computing, Graduate Surveys 1, 120

(learning Boolean functions, see also O'Donnell's book)

[18] J. Bruck and R. Smolensky. Polynomial threshold functions,ac0functions, and spectral norms.SIAM Journal on Computing, 21(1):3342, 1992

(approximate Boolean fucntions, see also O'Donnell's book for "concentration")

[19] M. Thornton, V. Nair, Efficient spectral coefficient calculation using circuit output probabilities, Digital Signal Processing 4 (4) (1994) 245 254.

(BDD, SDD and circuit output probability)

[20] E.M. Clarke, K.L. McMillan, X. Zhao, M. Fujita, and J. Yang, Spectral transforms for large Boolean functions with applications to technology mapping, DAC-30: ACM/IEEE Design Automation Conference, Dallas, TX, June 1993, pp. 5460 (BDD to SDD)

[21] Johan Hastad. Some optimal inapproximability results. Journal of the ACM, 48(4):798859, 2001 (Hastad's Theorem)