Balanced Splittable Hadamard Matrices

Jonathan Jedwab

Department of Mathematics, Simon Fraser University

Joint work with

Shuxing Li and Sam Simon, Simon Fraser University

Shuxing Li

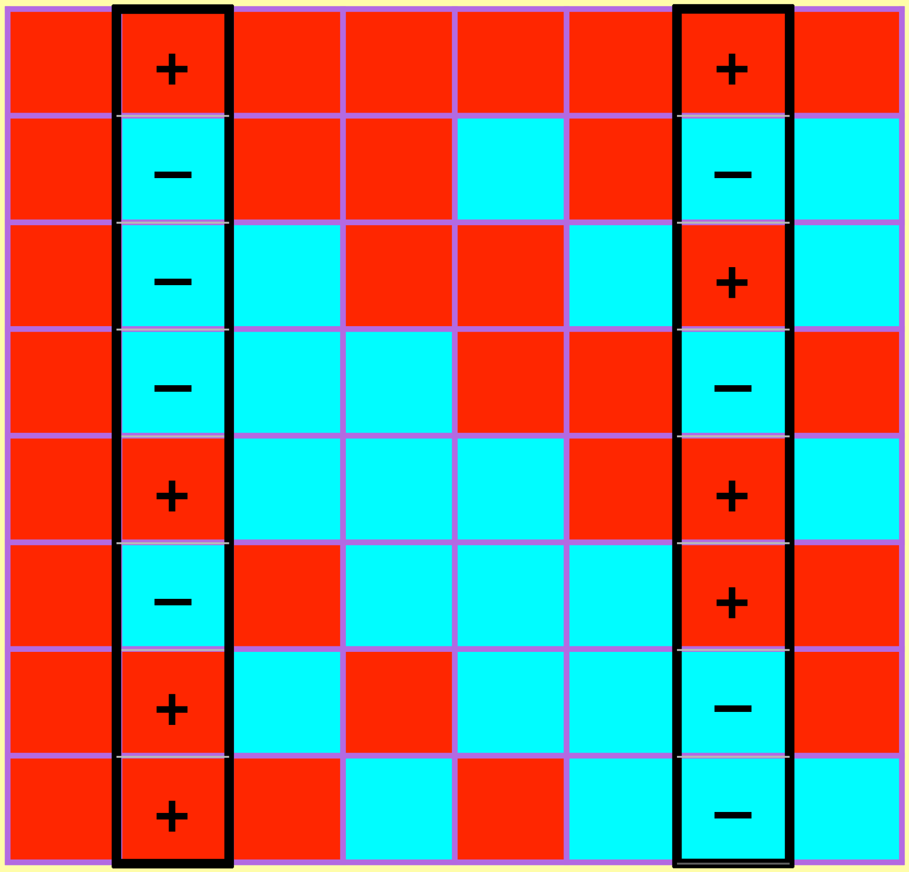
Sam Simon *

Jonathan Jedwab
1 August 2022

Outline

- Hadamard matrix
- Motivation and constructions
- Hadamard Matrix Conjecture
- Balanced splittable property
- Motivation
- Associated strongly regular graph
- Parameter classes
- Partial difference sets
- Multiple submatrices

Hadamard Matrix



Order 8 Hadamard matrix

dot product of every two distinct columns is 0

matches = # non-matches

Jonathan Jedwab
1 August 2022

Jacques Hadamard
1865 – 1963

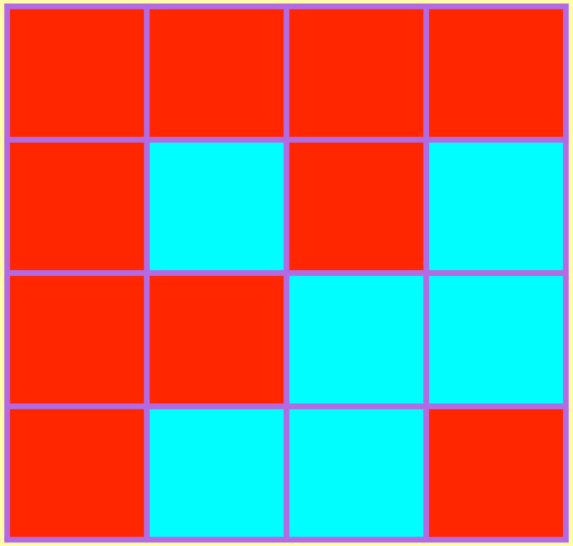
James Sylvester
1814 – 1897

Jonathan Jedwab
1 August 2022

Hadamard Matrix

- Order *n* Hadamard matrix *H*: entries in $\{+1,-1\}$, pairwise orthogonal columns
  - ⋆ $H^T H = nI_n$
  - ⋆ implies $HH^T = nI_n$, so also pairwise orthogonal rows

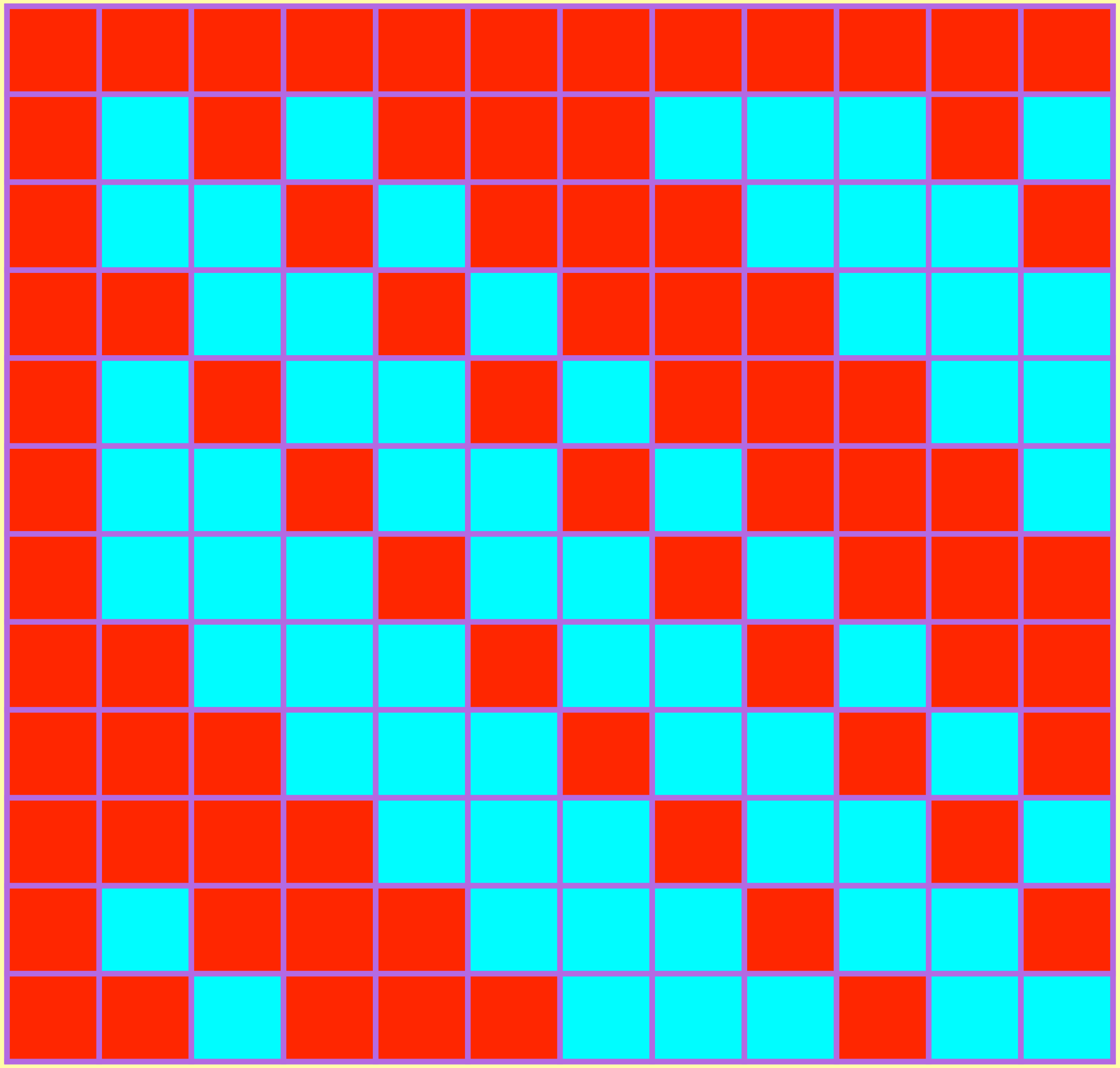
Examples



Order 4 Hadamard matrix

Jonathan Jedwab
1 August 2022

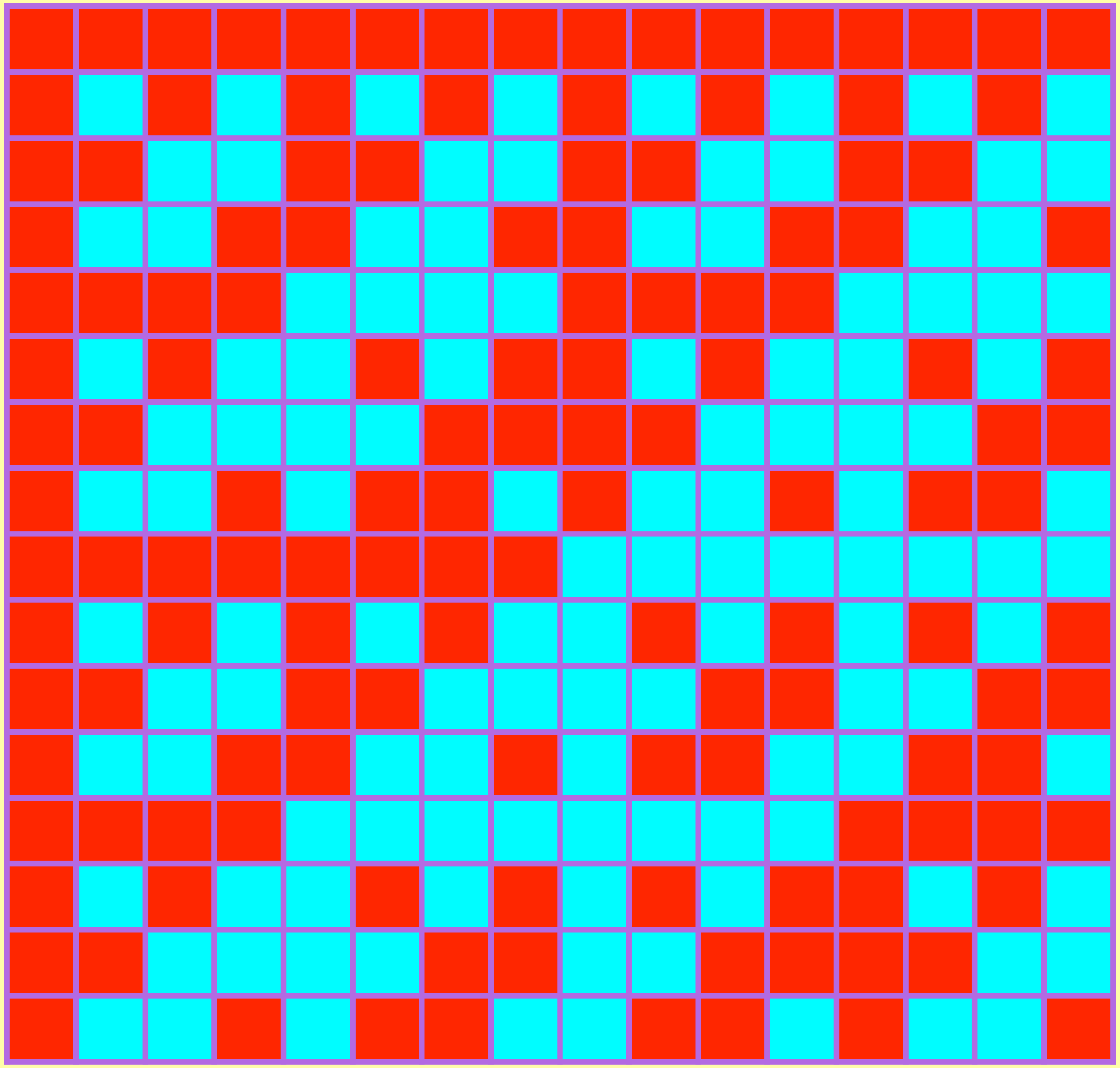
Examples



Order 12 Hadamard matrix

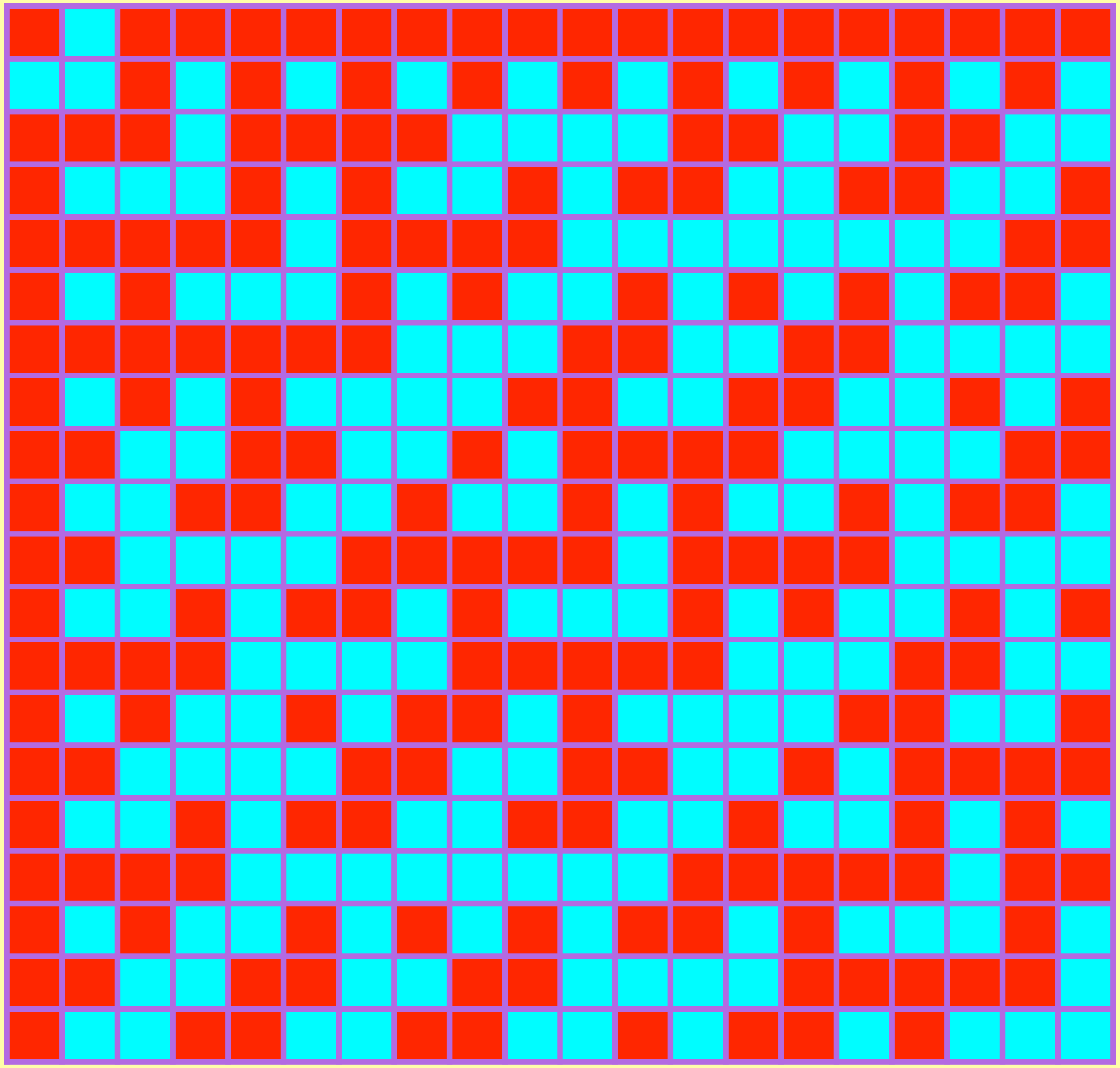
Jonathan Jedwab
1 August 2022

Examples



Order 16 Hadamard matrix

Examples



Order 20 Hadamard matrix

Jonathan Jedwab
1 August 2022

Motivation

- Theoretical importance: Hadamard matrices solve the maximum determinant problem for complex-valued matrices whose entries have magnitude at most 1

- Practical importance: applications include
  - ⋆ statistical designs: analyse experimental data to determine which quantities depend on others
  - ⋆ coding of digital signals: make messages easy to recover
  - ⋆ cryptography: make messages difficult to recover

Hadamard Matrix

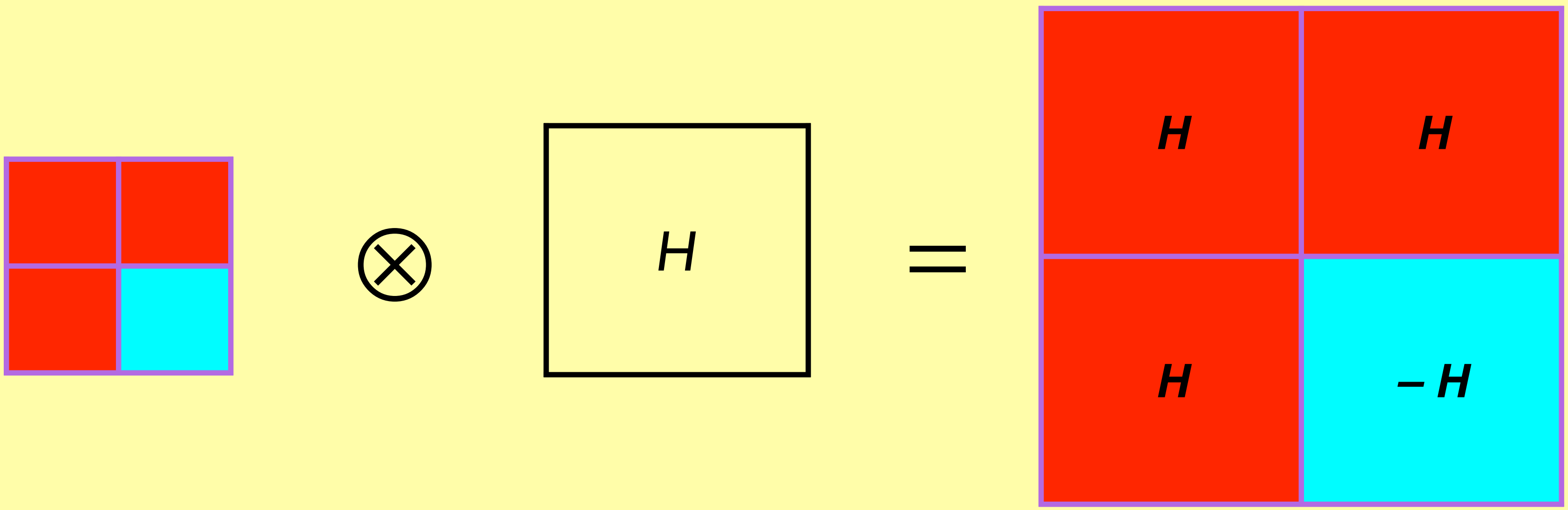
- Order n Hadamard matrix H: entries in $\{+1, -1\}$, pairwise orthogonal columns
  - ⋆ $H^T H = nI_n$
  - ⋆ implies $HH^T = nI_n$, so also pairwise orthogonal rows

- If $n > 2$, then $n = 4r$ for some positive integer r
  - ⋆ Conjecture (Paley 1933). There is a Hadamard matrix of order $4r$ for every positive integer r

Raymond Paley
1907 – 1933

Jonathan Jedwab
1 August 2022

Sylvester 1867: Doubling



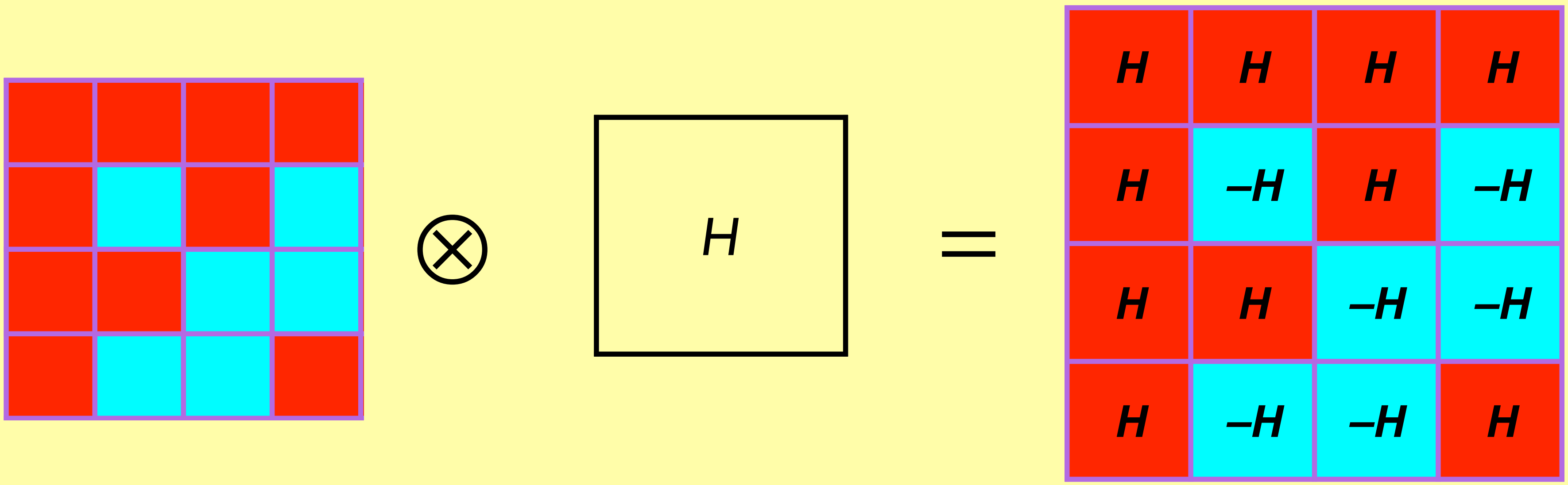
Hadamard matrix order 2

Hadamard matrix order *n*

Hadamard matrix order 2*n*

Jonathan Jedwab
1 August 2022

Hadamard 1893: Product



Hadamard matrix order *m*

Hadamard matrix order *n*

Hadamard matrix order *mn*

Jonathan Jedwab
1 August 2022

Hadamard Matrix Conjecture

Date	Order of smallest unsolved case becomes	Construction of previous smallest unsolved case by	Using computer?
1867	12	Sylvester	No
1893	28	Hadamard	No
1933	92	Paley	No
1962	116	Baumert, Golomb, Hall	Yes
1966	188	Baumert	Yes (?)
1975	268	Turyn	Yes
1985	428	Sawade	Yes
2005	668	Kharaghani, Tayfeh-Rezaie	Yes

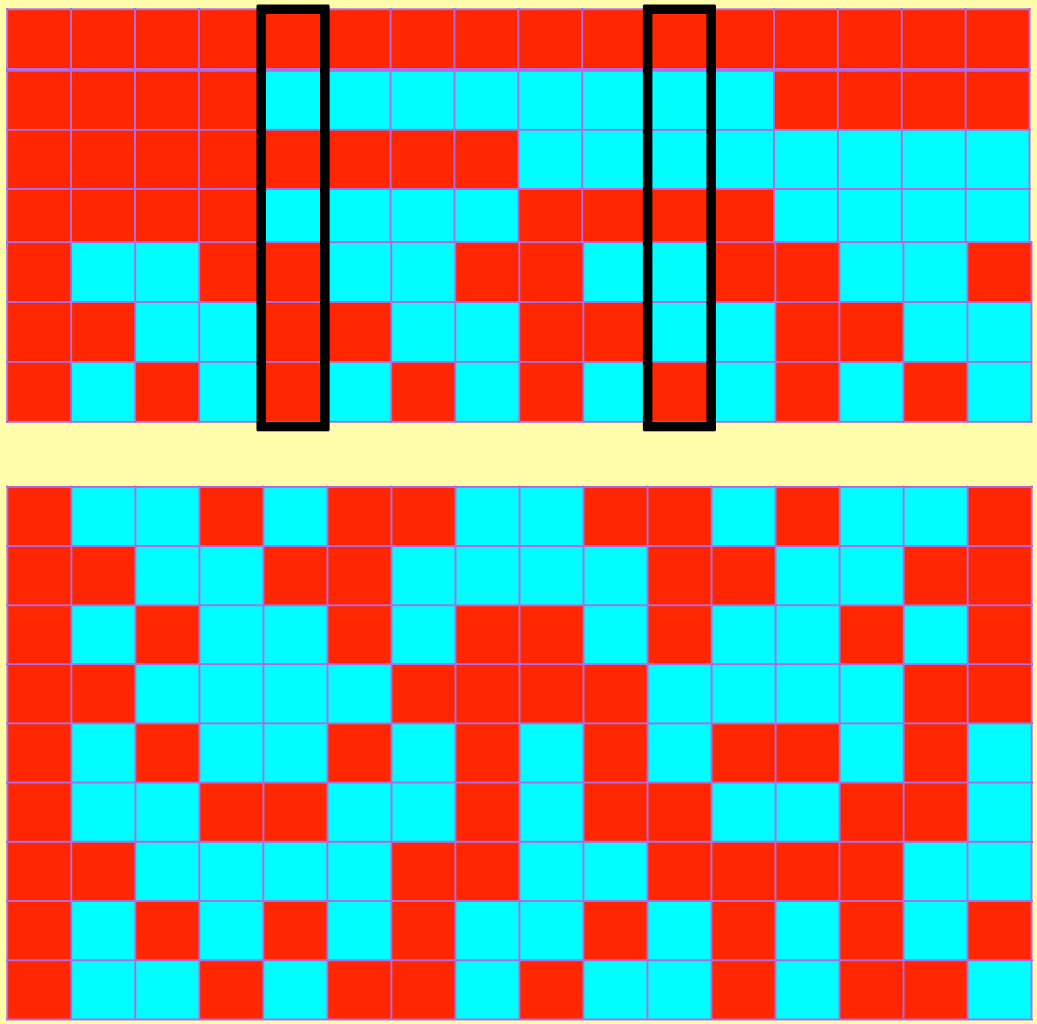
Jonathan Jedwab
1 August 2022

Solomon Golomb 1932 – 2016,
Leonard Baumert, Marshall Hall Jr. 1910 – 1990

Jonathan Jedwab
1 August 2022

Balanced Splittable

balanced splittable $(16, 7, 3, -1)$ Hadamard matrix



dot product
of distinct
columns is
3 or -1

Jonathan Jedwab
1 August 2022

Balanced Splittable

balanced splittable (n, ℓ, a, b) Hadamard matrix

H_1 (ℓ rows)

dot product of distinct columns is a or b

($n - \ell$ rows)

$$H_1^T H_1 = \ell I_n + a A + b(J_n - I_n - A)$$

Jonathan Jedwab
1 August 2022

Balanced Splittable

- "Balanced splittable" coined by Kharaghani & Suda (2019)
- Earlier equivalent formulations using
  - ⋆ real flat equiangular tight frames
  - ⋆ regular spherical two-distance sets
  - ⋆ two-distance tight frames

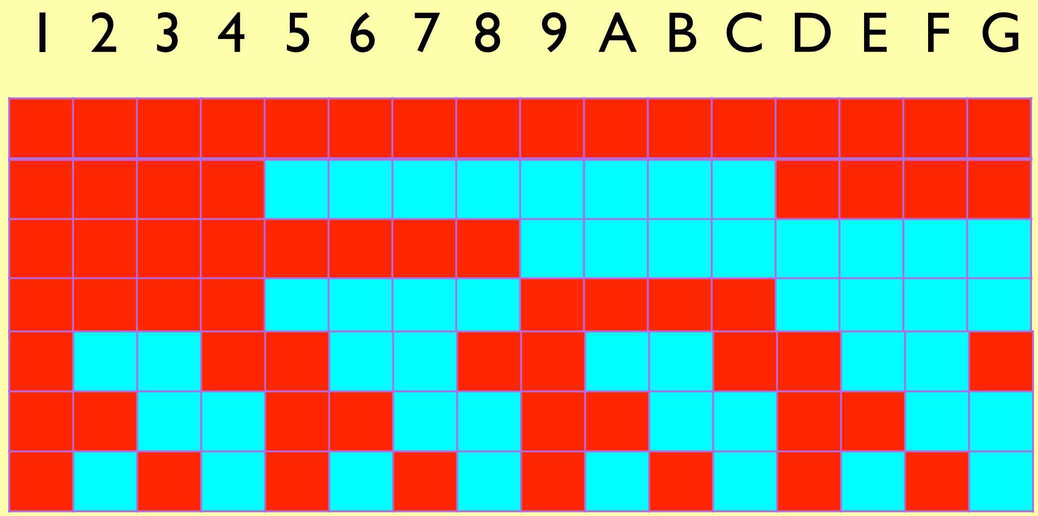
For which parameters (n, ℓ, a, b) is there a balanced splittable Hadamard matrix ?

Motivation

- Theoretical importance: balanced splittable property identifies subclass of Hadamard matrices with additional structure
  - ⋆ connections to strongly regular graphs
  - ⋆ new insights for Hadamard Matrix Conjecture ?

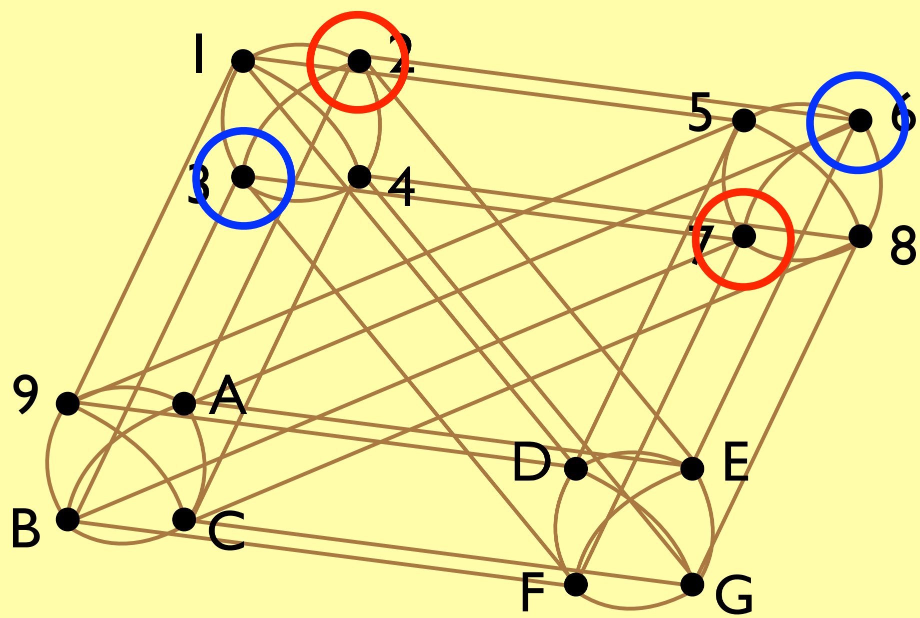
- Practical importance: new opportunities for advantageous signal design
  - ⋆ dot products of columns of submatrix are tightly controlled

Associated Strongly Regular Graph



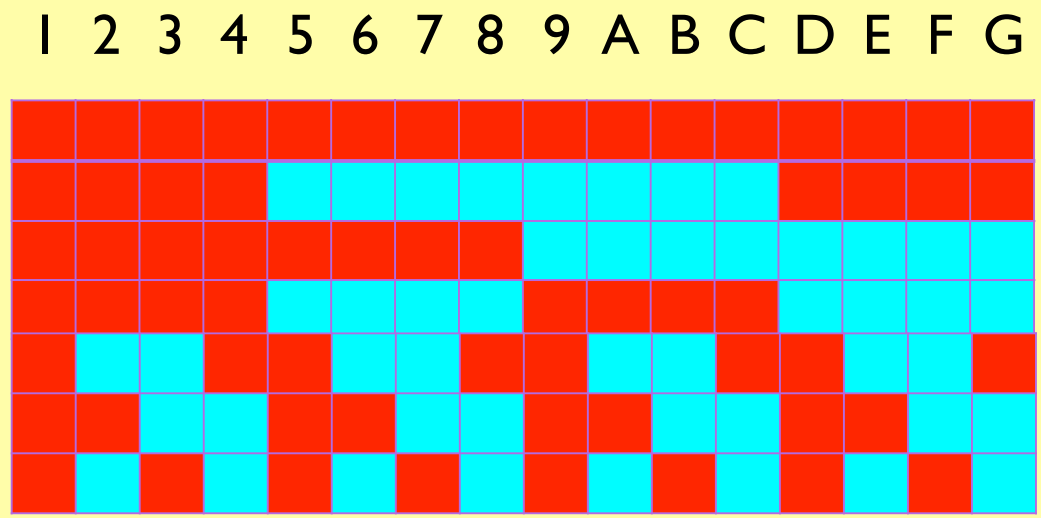
dot product of distinct columns is 3 or -1

(16,6,2,2) strongly regular graph

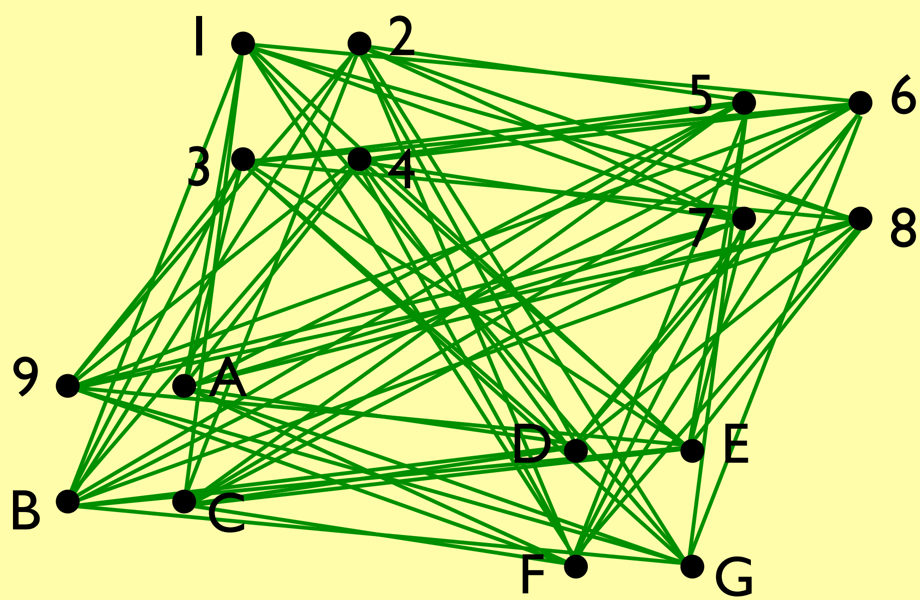


Jonathan Jedwab
1 August 2022

Associated Strongly Regular Graph



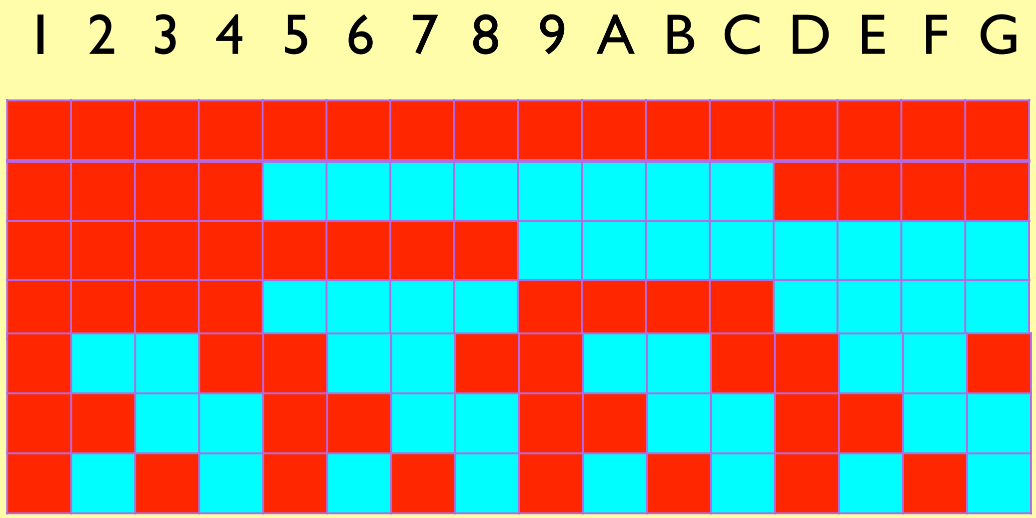
dot product of distinct columns is 3 or -1



(16, 9, 4, 6) strongly regular graph

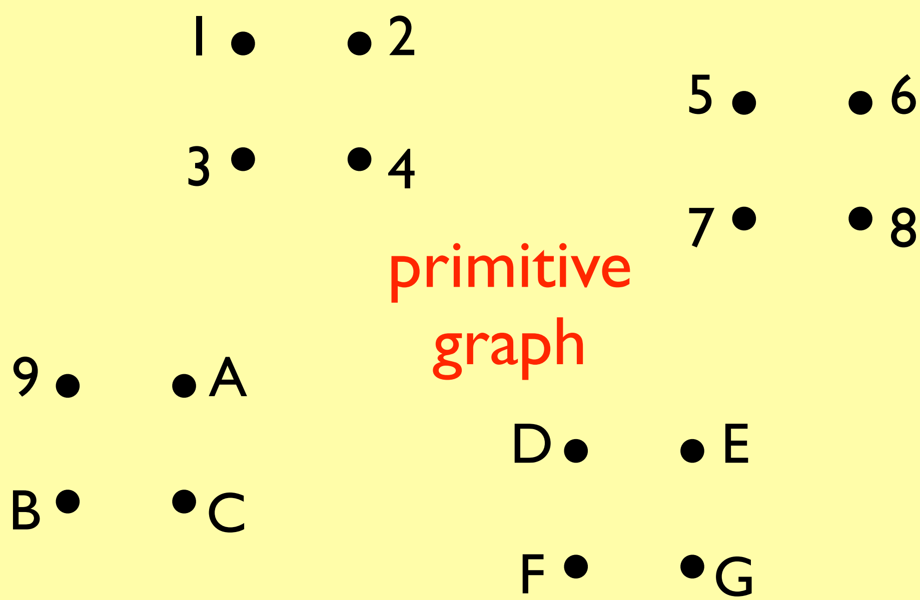
Jonathan Jedwab
1 August 2022

Associated Strongly Regular Graph



dot product of distinct columns is 3 or –1

(16,6,2,2) strongly regular graph (connected)



primitive graph

(16,9,4,6) strongly regular graph (connected)

Jonathan Jedwab
1 August 2022

Parameter Classes

- Jedwab, Li, Simon (2022+). Six classes of parameters (n, ℓ, a, b) of balanced splittable Hadamard matrix, according to
  - ⋆ $\ell = 2$?
  - ⋆ $b = -a$?
  - ⋆ $H_1 \mathbf{1} = \mathbf{0}$?
  - ⋆ is associated strongly regular graph primitive ?

Parameter Classes

- For example, for $\ell > 2$ and $b \neq -a$ and $H_1 \mathbf{1} = \mathbf{0}$:
  - ⋆ if associated graph G primitive then

$$n = \frac{(\ell - a)(\ell - b)}{\ell + ab} \qquad \ell \equiv a \equiv b \pmod{4}$$

$$\frac{\ell - b}{b - a}, \quad \frac{n}{b - a}, \quad \frac{n(b+1)}{2(b-a)}, \quad \frac{nb(b+1)}{(b-a)^2} \text{ are integers}$$

  - ⋆ if G not primitive then $(n, \ell, a, b) = (4rs, 4s-1, 4s-1, -1)$ for integers r and s, and G is disjoint union of $4s$ copies of complete graph K_r

Partial Difference Set

	0 0	
	0 0	0 1
	1 0	1 1

	0 1	
	0 0	0 1
	1 0	1 1

	1 0	
	0 0	0 1
	1 0	1 1

	1 1	
	0 0	0 1
	1 0	1 1

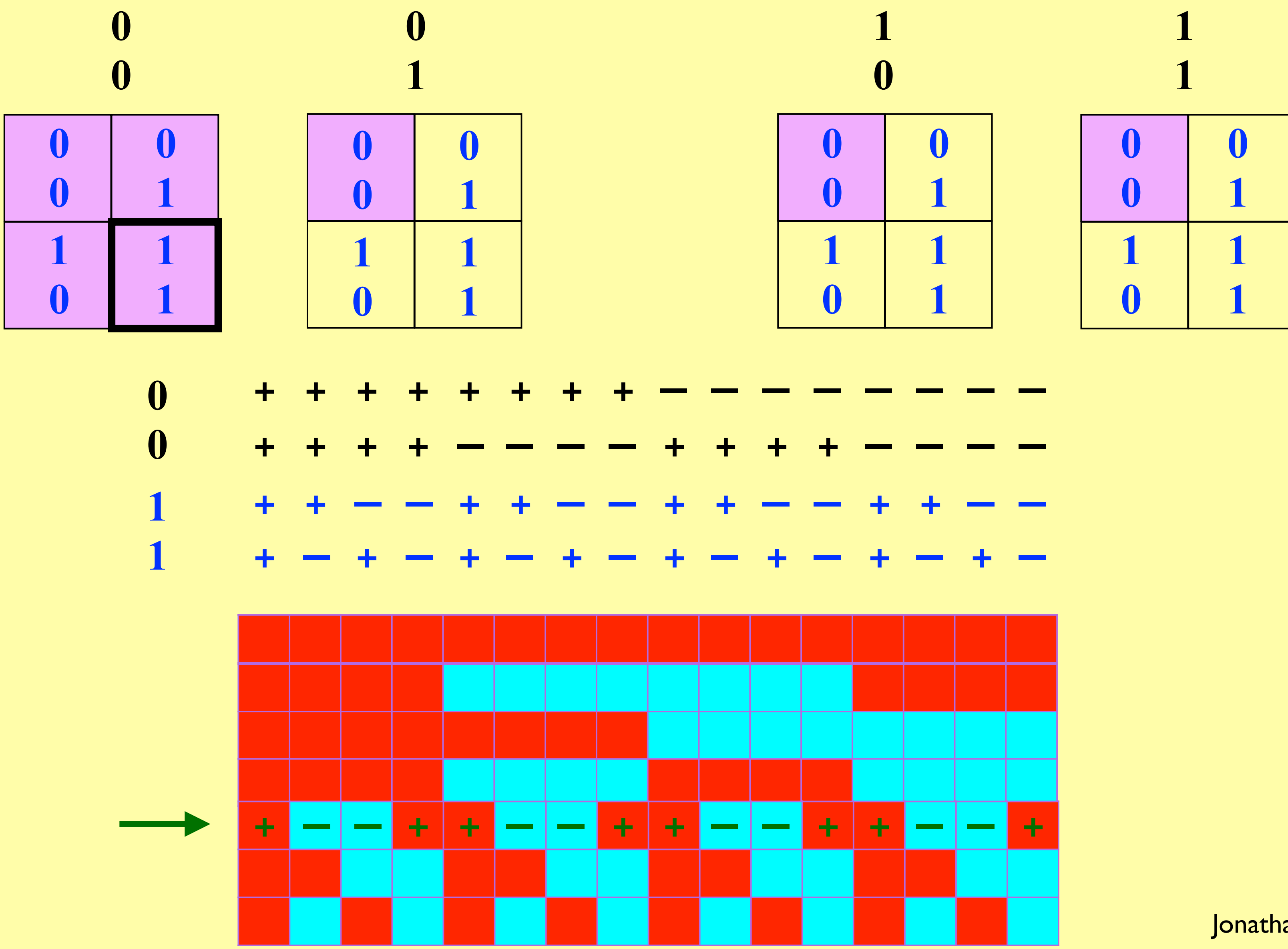
0	0	0	0	0	1	1
0	0	0	0	1	0	1
0	0	1	1	0	0	0
0	1	0	1	0	0	0

(16, 7, 4, 2) partial difference set in $\mathbb{Z}_2^4$

0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	4	4	4	4	2	2	2	4	2	2	2	4	2	2	2

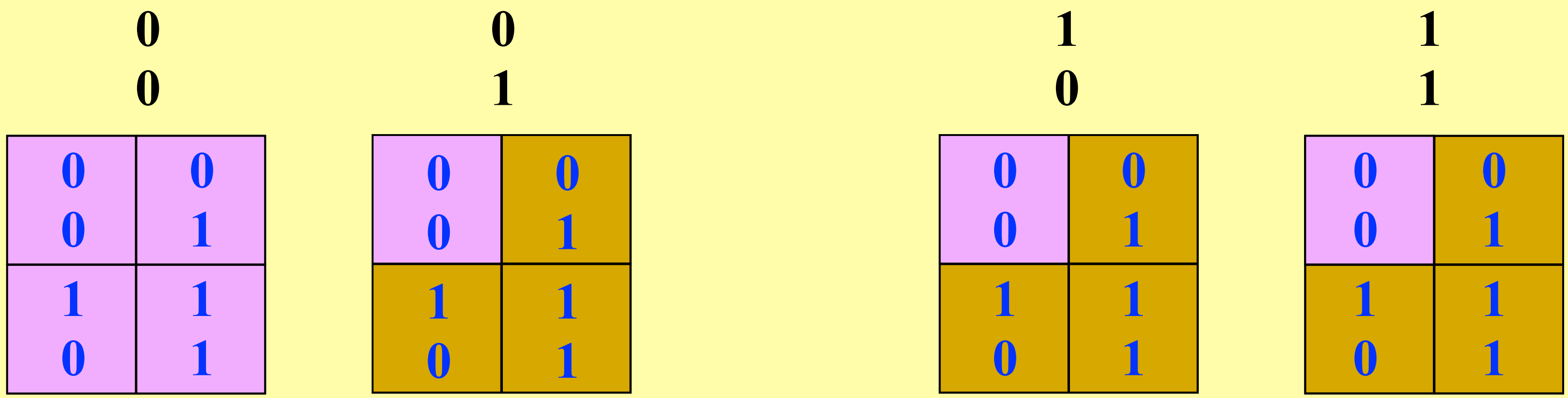
Jonathan Jedwab
1 August 2022

Partial Difference Set



Jonathan Jedwab
1 August 2022

Partial Difference Set



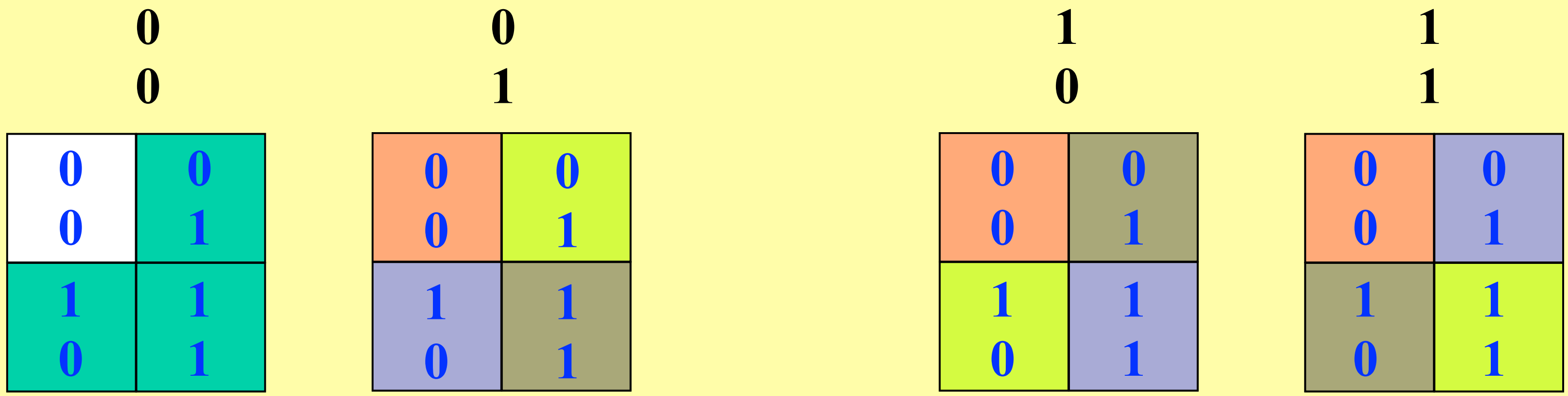
(16, 7, 4, 2) partial difference set in $\mathbb{Z}_2^4$

↕

balanced splittable (16, 7, 3, -1) Hadamard matrix

Jonathan Jedwab
1 August 2022

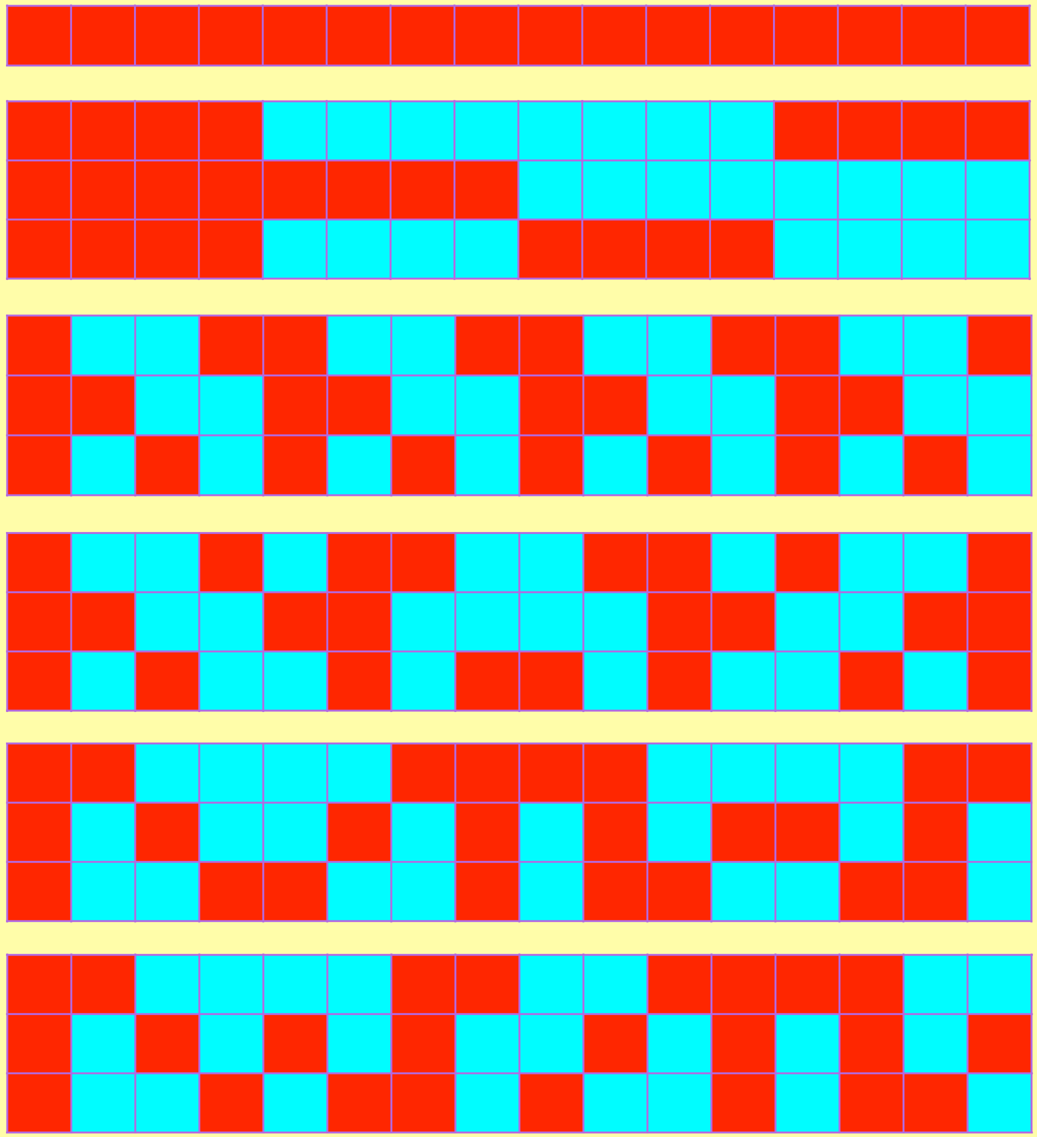
Partial Difference Set



- Can partition the elements of $\mathbb{Z}_2^4$ into 6 subsets: the zero element, and five (16, 3, 2, 0) partial difference sets

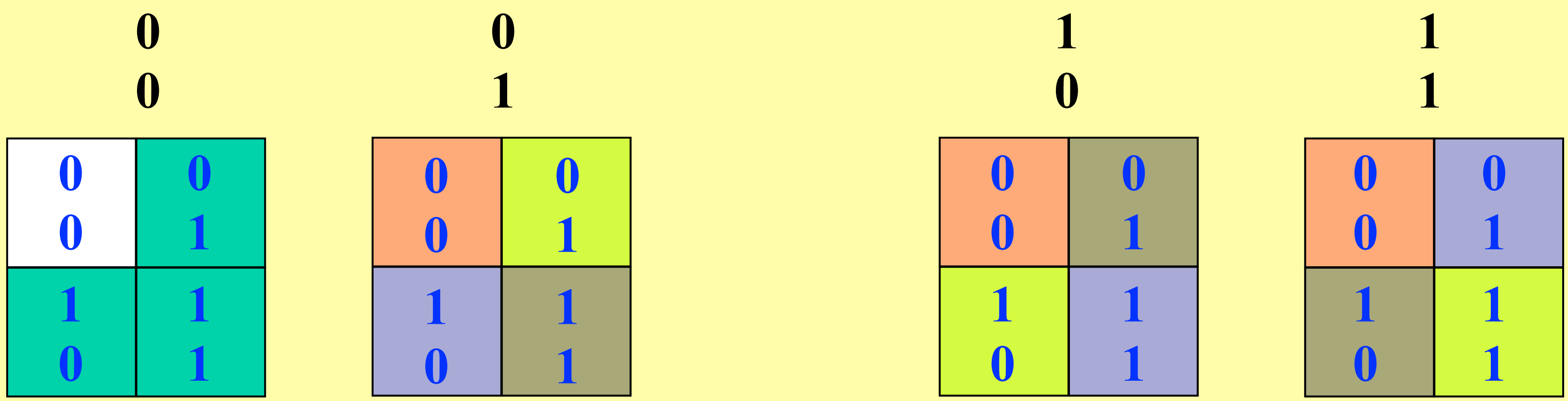
Jonathan Jedwab
1 August 2022

Multiple Submatrices



Jonathan Jedwab
1 August 2022

Partial Difference Set



- Can partition the elements of $\mathbb{Z}_2^4$ into 6 subsets: the zero element, and five (16, 3, 2, 0) partial difference sets

- Every union of the 6 subsets is also a partial difference set !

Multiple Submatrices

partial difference set in $\mathbb{Z}_2^4$

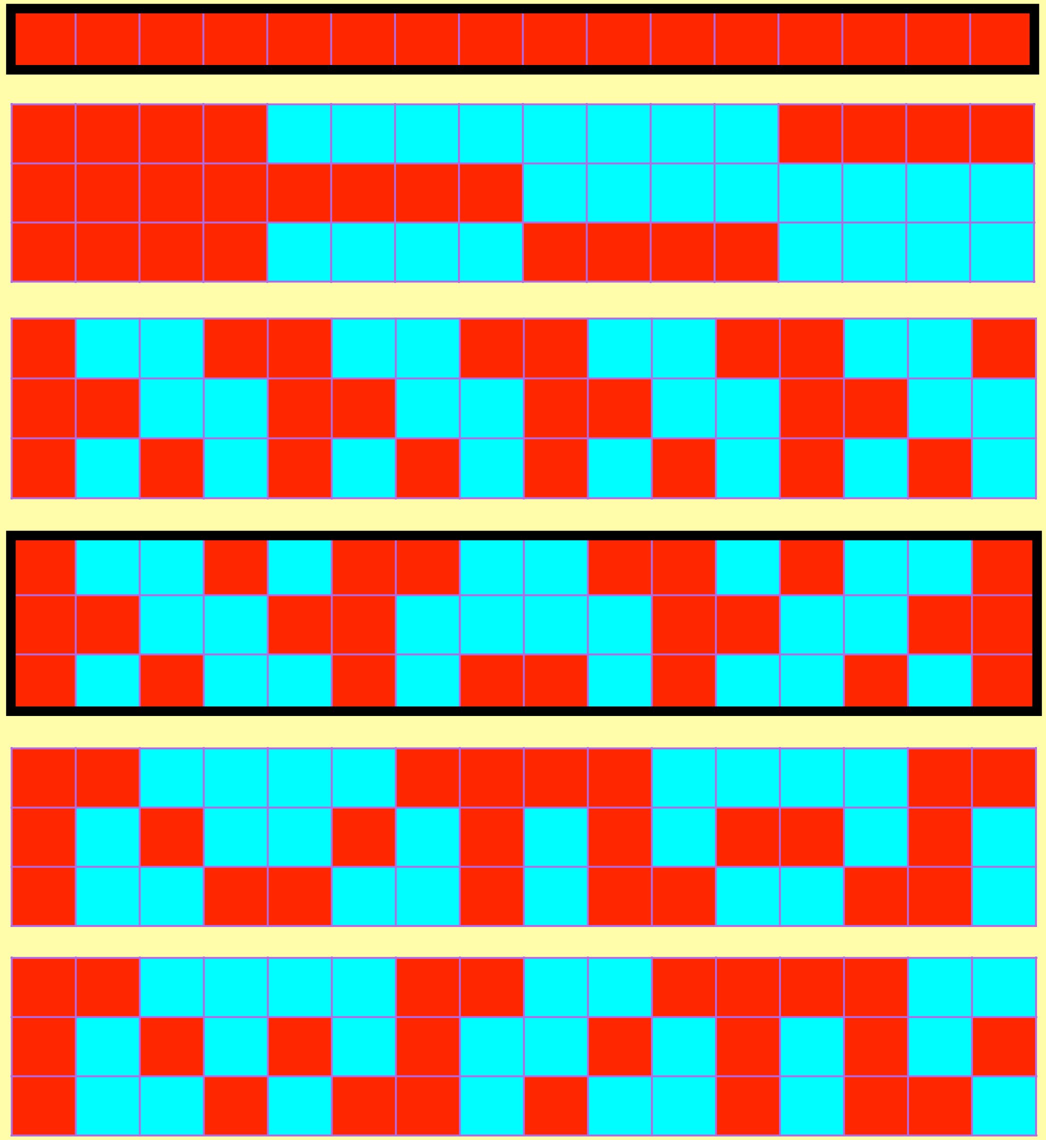
(16, 4, 4, 0)

balanced splittable Hadamard matrix

(16, 4, 4, 0)

Jonathan Jedwab
1 August 2022

Multiple Submatrices



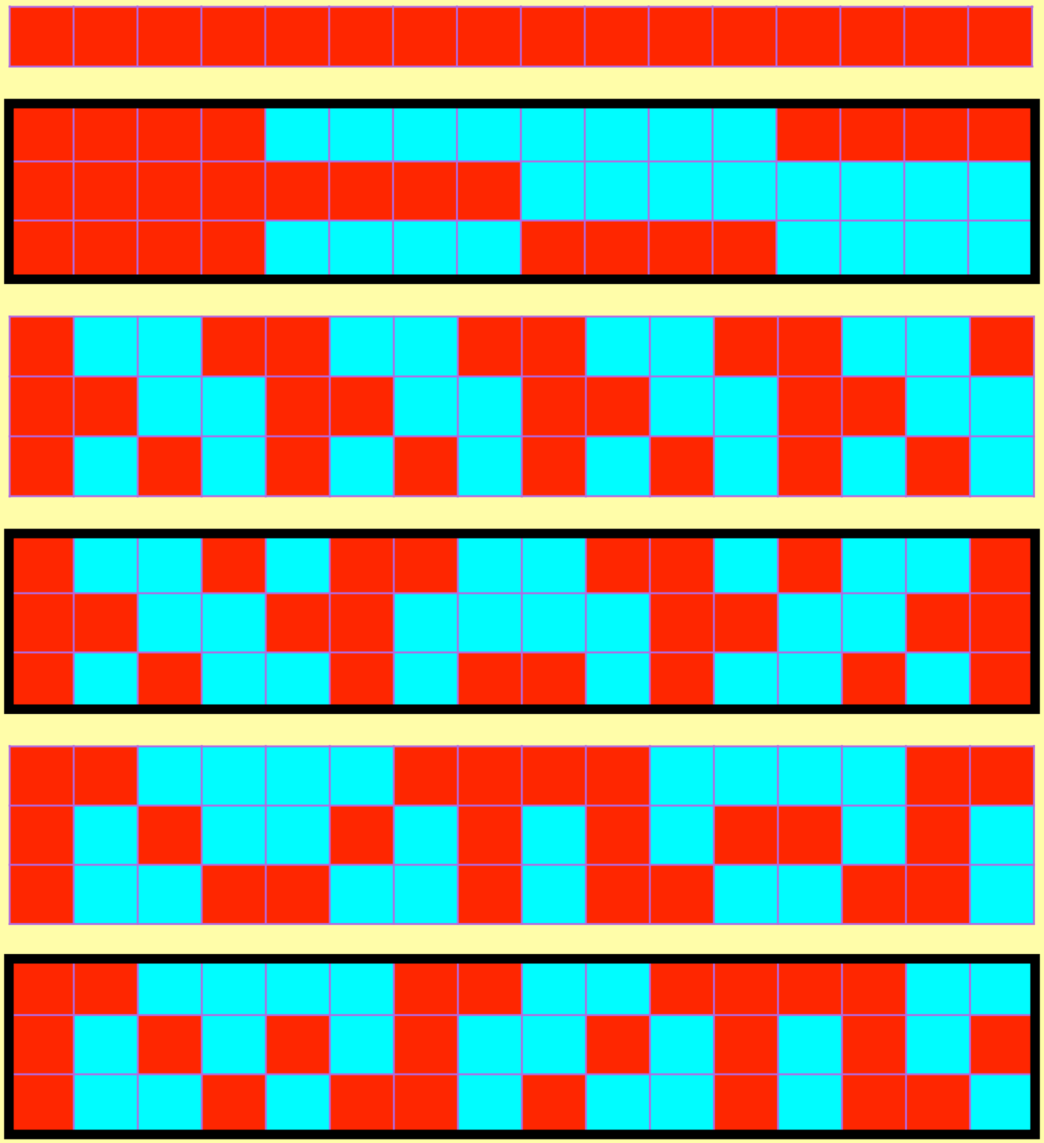
dot product
of distinct
columns is
4 or 0

Jonathan Jedwab
1 August 2022

Multiple Submatrices

partial difference set in $\mathbb{Z}_2^4$	balanced splittable Hadamard matrix
(16, 4, 4, 0)	(16, 4, 4, 0)
(16, 6, 6, 2)	(16, 6, 2, -2)
(16, 7, 4, 2)	(16, 7, 3, -1)
(16, 9, 4, 6)	(16, 9, 1, -3)

Multiple Submatrices



dot product of distinct columns is 1 or –3

Jonathan Jedwab
1 August 2022

Multiple Submatrices

- Jedwab, Li (2021). Polhill (2009). Polhill Davis Smith (2013). Construct packings of partial difference sets by partitioning the elements of $\mathbb{Z}_2^{2m}$ into $r+1$ subsets: the zero element, and r partial difference sets so that every union of the $r+1$ subsets is also a partial difference set

- Jedwab, Li, Simon (2022+). Use to construct Hadamard matrices that are balanced splittable with respect to multiple submatrices simultaneously