Applications of Combinatorial Designs to Wireless Mesh Networks

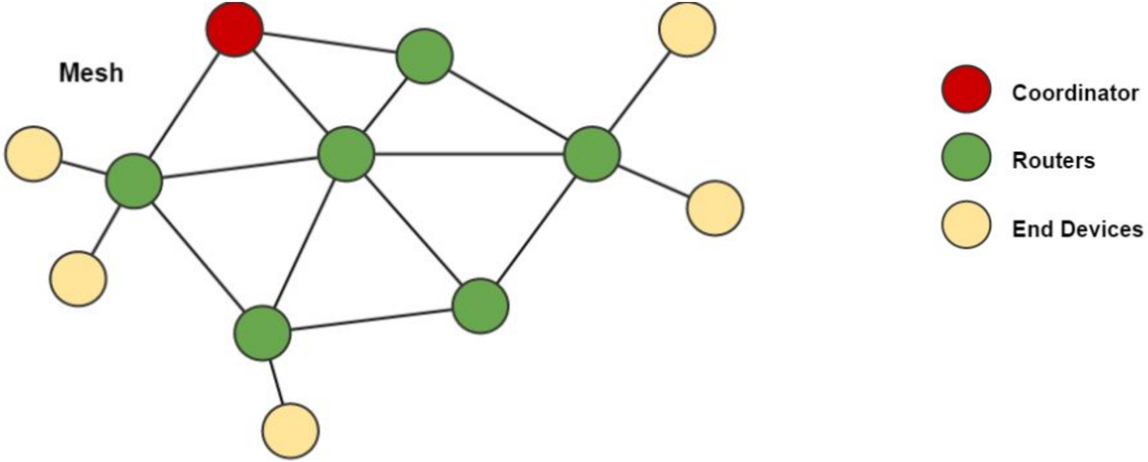
Daniel Connolly, Anusha Datar, Emma Westerhoff

Application 1: Asynchronous wakeups of wireless mesh networks

- **Application 1: Asynchronous wakeups of wireless mesh networks**
- Application 2: Key distribution in wireless mesh networks

Introduction

- A **wireless mesh network** is a communications network made up of radio nodes organized in a mesh topology (rich interconnection)
- Problem Statement: How do we transmit data across a network while limiting the amount of time any node is on?



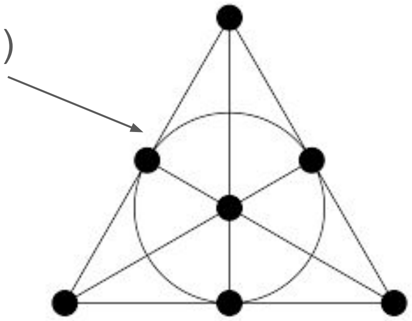
Properties of successful schedule

- Different power states
  - ON: ~200 mA
  - OFF: ~0.5 mA
- Maintain network connectivity regardless of the power states nodes may be in
- Synchronous: All wake up every ? seconds
  - Required to sync to a common clock
  - All devices are on longer than they need to be
- Asynchronous: Intelligent design
  - Much harder to implement
  - Increased battery life
  - Schedule can be constructed with **symmetric designs**

Block Designs: (v,b,r,k,λ)

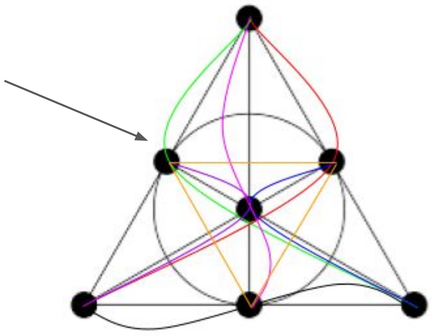
- **Balanced**: Each pair of points appear together λ times
- **Incomplete**: Cannot fit all points in each block
- **Symmetric**: Equal number of points and blocks (v=b and r=k)

(7,7,3,3,1)



Symmetric

(7,14,6,3,2)



Asymmetric

v
points (number of elements)

b
number of blocks

r
number of blocks containing a given point

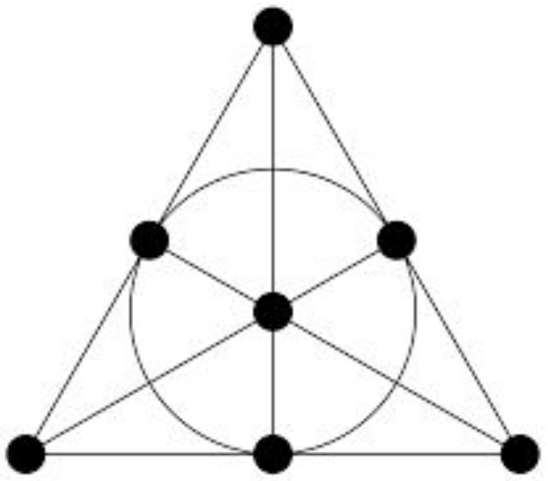
k
number of points in a block

λ
number of blocks containing any 2 (or more generally *t*) distinct points

Projective Plane IS a SBIBD

- On a **projective plane**:
  - Any two distinct nodes occur in a unique time block.
  - Any pair of distinct time blocks intersect in a unique node.
  - There exist three nodes that are not awake during the same time block (non-collinear)
- Used to represent block designs with *λ=1*

Projective Plane



Construction of the Projective Plane: Approach 1

Difference Sets

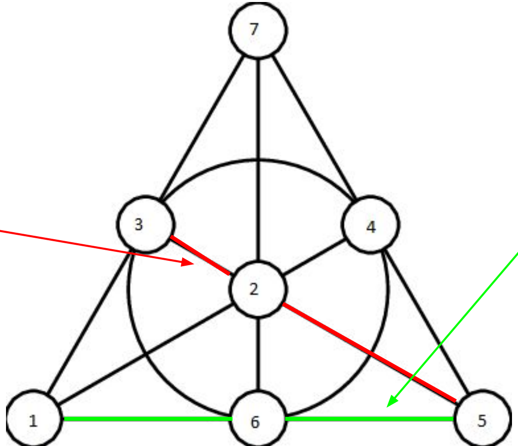
Difference Sets

- Finding projective planes: 7 nodes
  - Generate difference set

	1	**2**	**4**
1	0	1	3
2	6	0	2
4	4	5	0

  - Generate projective plane from difference set

1 ***+1*** = 2
1 ***+2*** = 3
1 ***+4*** = 5



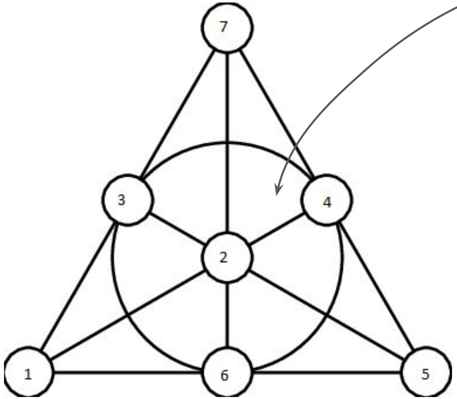
4 ***+1*** = 5
4 ***+2*** = 6
4 ***+4*** (mod 7) = 1

Asynchronous Scheduling Using (v,k,λ) design

Objective: Given v, minimize k_u

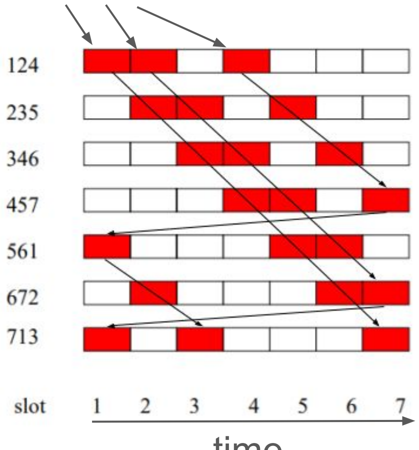
- Map symmetric block design to symmetric wakeup schedule function
- Symmetric: all nodes have same duty cycle

v
total number of time slots
k_u
time slots in which a node u is awake every v slots



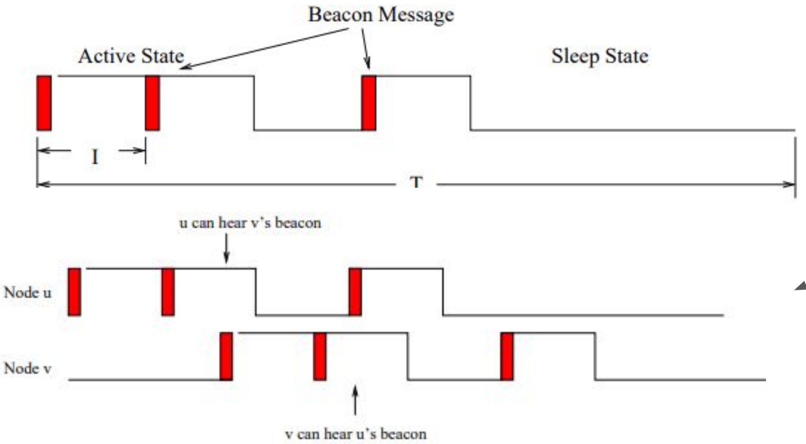
(7,3,1)-design

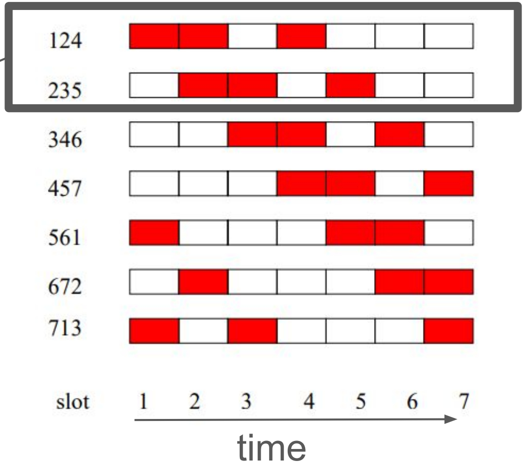
{1,2,4} difference set!



Application / Behavior of (v,k,λ) design

- Objective: Minimize amount of time any node is on (power management)
- Even with a shift in clock cycles (within reason), any two nodes can still communicate



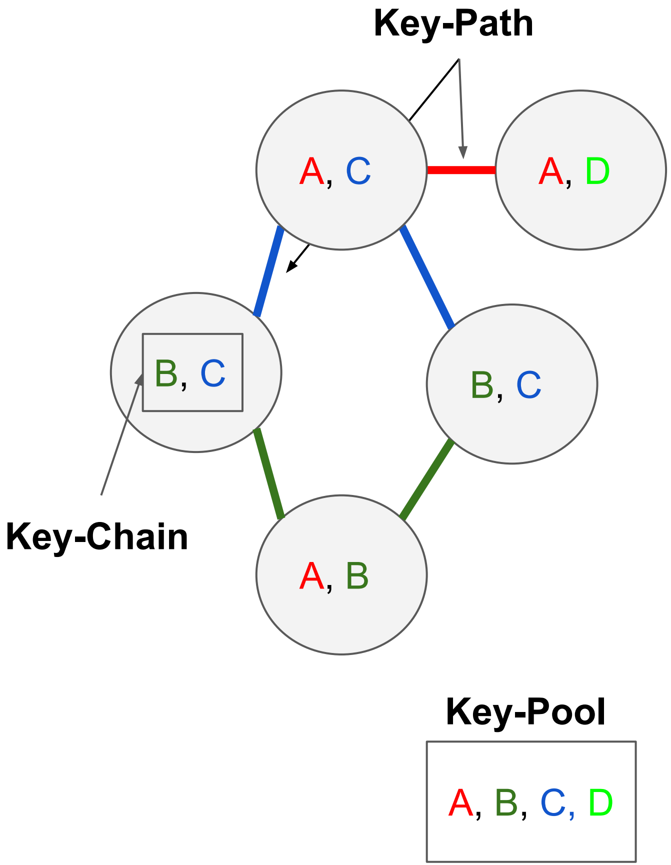


Application 2: Key distribution in wireless mesh networks

- Application 1: Asynchronous wakeups of wireless mesh networks
  - Introduction
  - Properties of successful schedule
  - Block Designs (v,b,r,k,λ)
  - Projective Plane
  - Difference Sets
  - Asynchronous scheduling using (v,k,λ) design
  - Application and behavior
- **Application 2: Key distribution in wireless mesh networks**

Introduction

- Each node has a preloaded **key-chain** of selected keys from a **key-pool**
- Neighboring nodes must have a **shared key** and nodes communicate along a **key-path**
- Goal: minimize the length of the key-path given memory and security constraints

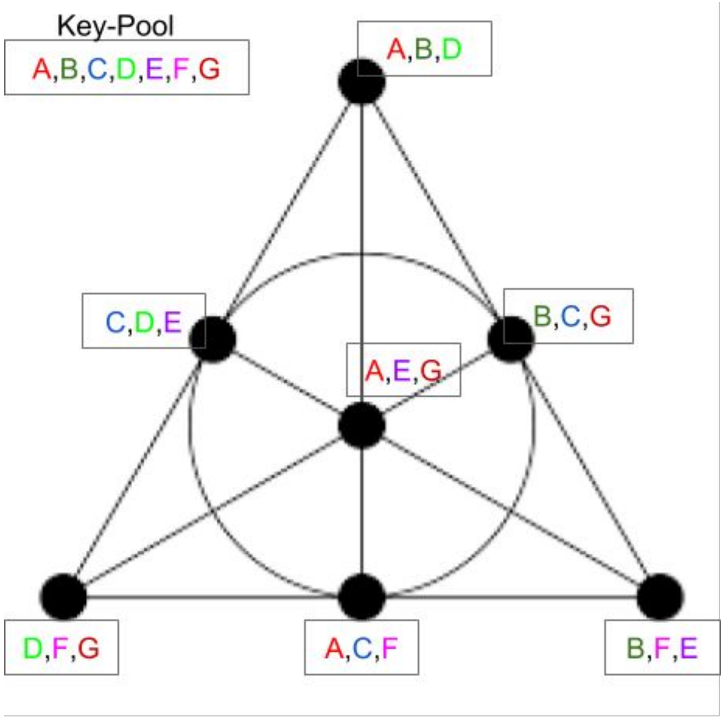


Approaches to Key Distribution

- **Symmetric Designs**
- Generalized Quadrangle

Symmetric Designs

- Symmetric (v,k,λ)-design (7,3,1)



v
Sensor nodes / key-chains

k
Keys in each key-chain

λ
Number of keys each pair of key-chains share

Construction of the Projective Plane: Approach 2

MOLS

MOLS and Symmetric Designs

- A set $\{L_1, L_2, \ldots, L_k\}$ of Latin squares of the same order are called **mutually orthogonal Latin squares (MOLS)** if any two in the set are orthogonal mates
- For any prime power q, there are exactly q-1 MOLS
- Using MOLS, we can **quickly** construct a projective plane

MOLS and Symmetric Designs

- **Projective Plane**: a set of points such that every line is unique and each line contains at least three points

As an example consider the set of 3 MOLS of order 4:

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

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

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

Now, let A be the matrix,

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Lines of the projective plane (size 20) are

- 4: Rows of A ({1,2,3,4}, {5,6,7,8}...)
- 4: Columns of A ({1,5,9,13},{2,6,10,14}...)
- 12: Columns of Latin Squares superimposed on A
    - Column 1 of LS1: {1,2,3,4} -> {1,6,11,16}
    - Column 2 of LS1: {2,1,4,3} -> {2,5,12,15}
    - Column 1 of LS2: {1,3,4,2} -> {1,7,12,14}

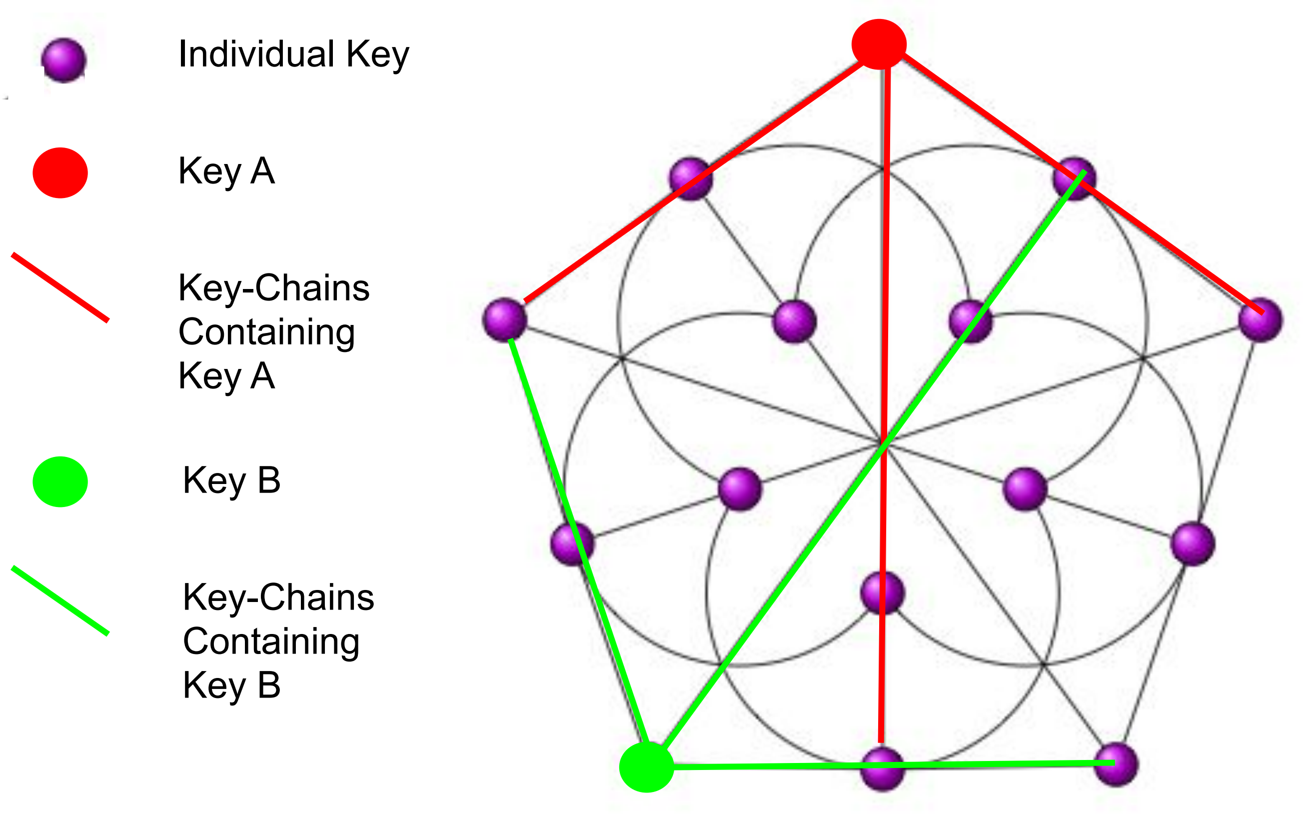
Symmetric Designs

- Simple to construct
- Probability of key-share is 1

Approaches to Key Distribution

- Symmetric Designs
- **Generalized Quadrangle**

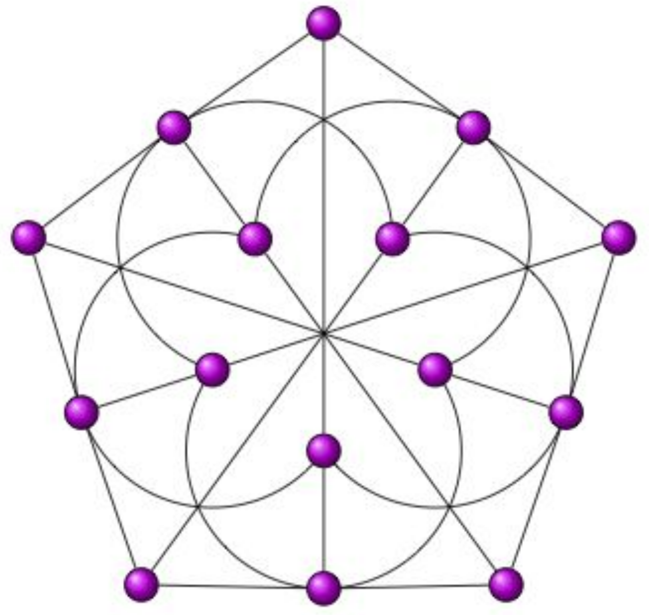
Generalized Quadrangle Key Distribution



Generalized Quadrangle

With a GQ(s, t):

- Each point is a key
- Each line is a key-chain for a node



GQ(2,2)
Key-pool size: 15
Nodes/keychains: 15

Performance

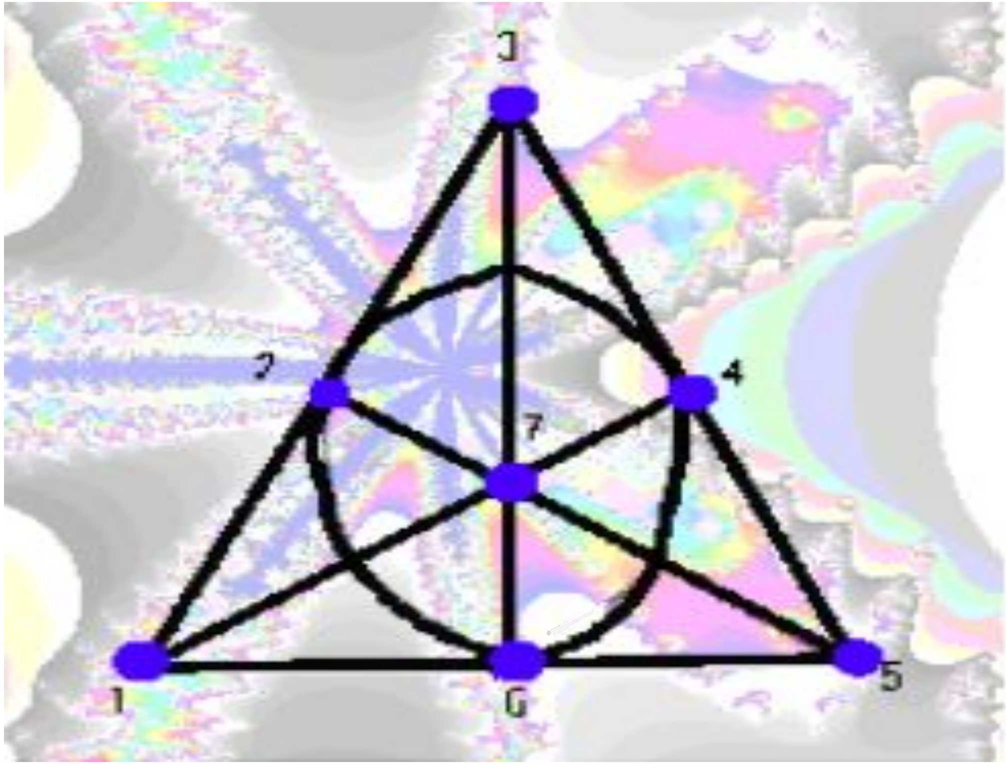
Metric	**Most Optimized Design**
Minimize Keys Per Node	Generalized Quadrangle
Maximize resilience	Generalized Quadrangle
Maximize probability two blocks have a shared key	Symmetric Design
Maximize simplicity for construction	Symmetric Design

Conclusion

- Application 1: Asynchronous wakeups of wireless mesh networks
- Application 2: Key distribution in wireless mesh networks
    - Introduction
    - Symmetric Designs
    - MOLS and Symmetric Designs
    - Generalized Quadrangle Design
    - Performance

Any Questions?

Thanks for listening!



Supplementary Materials

The following slides constitute our supplementary materials.

MOLS and Symmetric Designs

- A set $\{L_1, L_2, \ldots, L_k\}$ of Latin squares of the same order are called **mutually orthogonal Latin squares (MOLS)** if any two in the set are orthogonal mates
- For any prime power q, there are exactly q-1 MOLS
- Using MOLS, we can **quickly** construct a symmetric design of size v ($O(v^{1.5})$)

Algorithm Step	Run Time
Require: :v {total number of nodes}	
Find minimum prime power q such that $q^2+q+1 \geq v$	$O(?^?)$
Construct q-1 MOLS of order q	$O(q^3) \cong O(v^{1.5})$
Construct q^2 blocks of *affine plane* of order q	$O(v^{1.5})$
Affine Plane ⇒ *Projective Plane*	$O(v)$

Complementary Designs

The **complement** of a D(v, k, λ) design is:

$$D = (v, v-k, v-2k+\lambda)$$

For the Fano Plane (7, 3, 1) Design, the complement is a (7, 4, 2) design, and the complementary blocks of the design are {3, 4, 5, 6}, {1, 2, 5, 6}, {1, 2, 3, 4}, {0, 2, 4, 6}, {0, 2, 3, 5}, {0, 1, 4, 5}, and {0, 1, 5, 6}

Difference Sets

- A **cyclic (v,k,λ)-difference set** is a set $D=\{d_1,d_2, ...,d_k\}$ of <u>distinct</u> elements of Z_v such that each non-zero element $d \in Z_v$ can be expressed in the form $d=d_i-d_j \pmod v$ in precisely λ ways.
- Finding symmetric designs
  - Generate difference set
    - Small size
    - Minimize modulus
      - Minimum possible: s^2-s+1
  - Generate projective plane from difference set
    - Iterative for-loop approach

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

s rows

s-1 possible slots per row

Multiplier Theorem for Difference Sets

1. If p is a prime divisor of $n=k-\lambda$ with $p>\lambda$ and $(p,v)=1$, then p is a multiplier of D.
2. If D is a (v,k,λ) difference set in Z_v with $(v,k)=1$, then there exists a translate of D which is fixed by every multiplier of D.

Example:

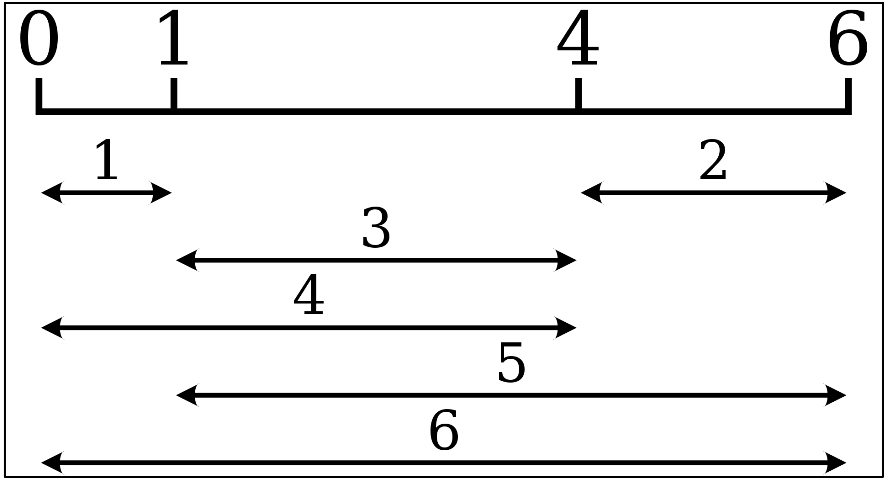
- 2 is a multiplier for the (7,3,1) difference set D={2,3,5}.
    - {2*2,2*3,2*5} mod 7 = {4,6,10} mod 7 = {3,4,6}

Golomb Ruler - Application of Difference Sets

Difference sets are closely related to Golomb rulers

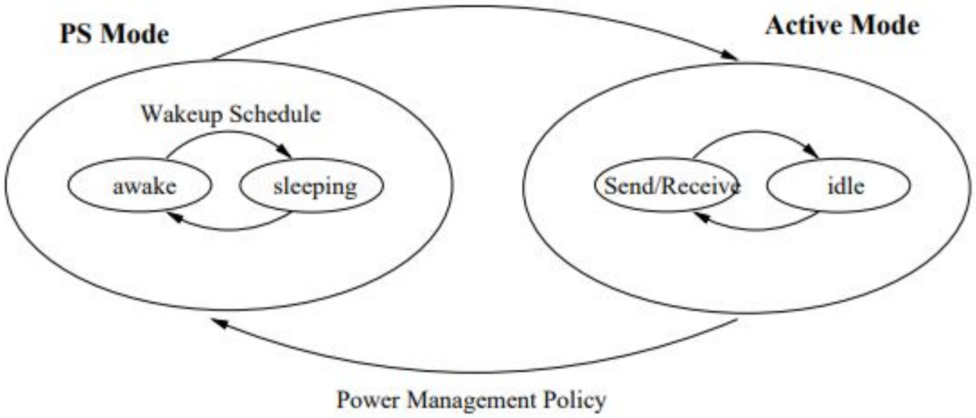
Golomb Ruler

- Set of marks at integer positions along an imaginary ruler such that no two pairs of marks are the same distance apart
- Number of marks on the ruler is its order, and the largest distance between two of its marks is its length

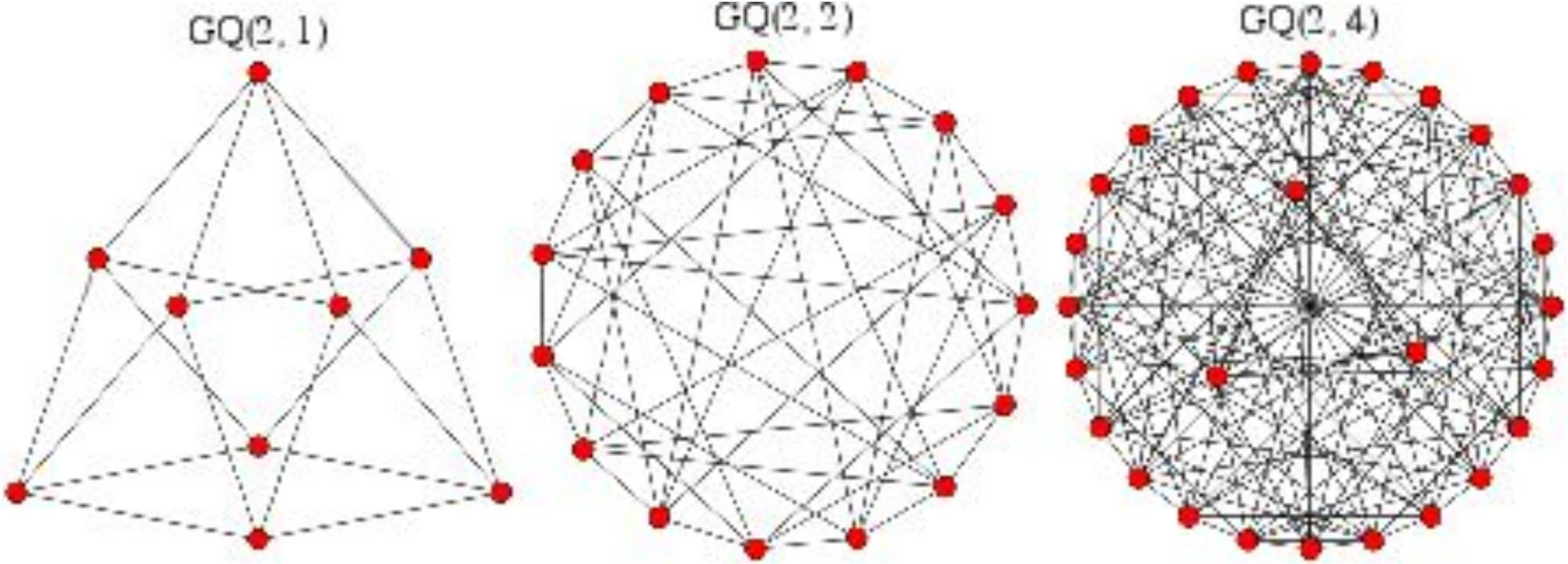


Power Management on top of scheduling

- On demand vs slot based



Visualization of GQ



Maximize number of blocks given block size

Symmetric Design

Symmetric designs are characterized by ($\mathbf{v}$=q^2+q+1, $\mathbf{k}$=q+1, $\boldsymbol{\lambda}$=1)

So, they will always have a ratio of number of blocks over number of points per block of

$$\frac{q^2+q+1}{q+1}$$

Generalized Quadrangle

The generalized quadrangle design GQ(q, q) has (q+1)(q^2+1) blocks per design and q + 1 points per block, so they will always have a ratio of:

$$\frac{(q+1)(q^2+1)}{q+1}$$

The GQ(q, q^2) design has the maximum number of blocks given a specific block size.

.

Minimize block size given number of blocks

Symmetric Design

Symmetric designs are characterized by ($\mathbf{v}$=q^2+q+1, $\mathbf{k}$=q+1, $\boldsymbol{\lambda}$=1)

So, they will always have a ratio of number of points per block over number of blocks of

$$\frac{\mathbf{q+1}}{\mathbf{q^2+q+1}}$$

Generalized Quadrangle

The generalized quadrangle design GQ(q, q) has (q+1)(q^2+1) blocks per design and q + 1 points per block, so they will always have a ratio of:

$$\frac{\mathbf{(q+1)(q^2+1)}}{\mathbf{q+1}}$$

The GQ(q^2, q^3) design has the minimum block size given the number of blocks.

.

Simplicity of Construction

Symmetric Design

When built using the MOLS-based construction method, this requires constructing a $q-1$ MOLS of order q, creating q^2 blocks of affine plane, and then converting the affine plane into the projective plane.

In total, this is a runtime of $O(q^3) = O(v^{1.5})$

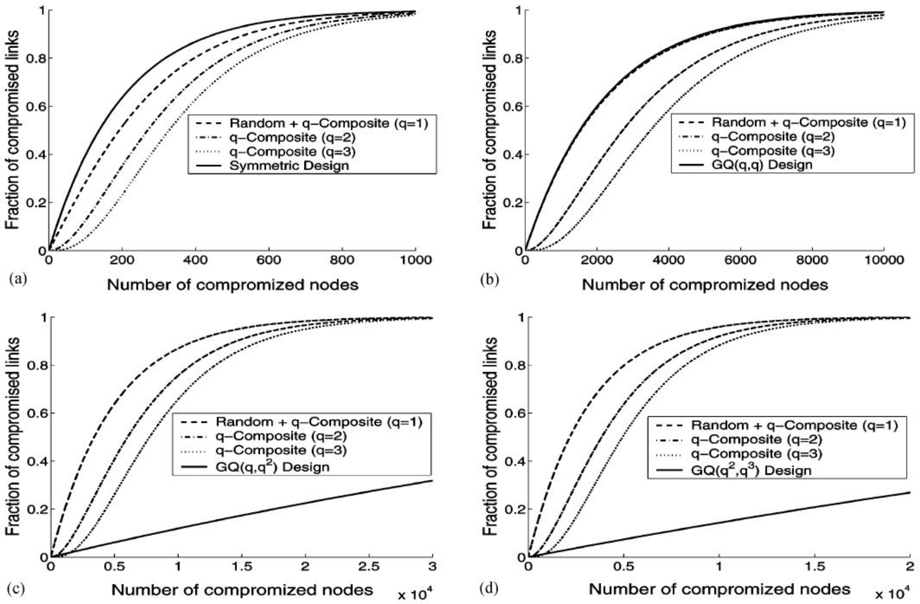
Generalized Quadrangle

The GQ construction algorithm requires finding the v points where $v = (s+1)(st+1)$ and then finding collinear points for each point and drawing lines between them.

In total, this is a runtime of $O(v^2)$

The symmetric design has a simpler construction runtime.

Maximize Resilience



The generalized quadrangle design, especially GQ(q^2, q^3), is the most resilient.

Maximize probability two blocks have a shared key

Symmetric Design

For a symmetric design, the probability that any pair of blocks share a key is equal to **1**.

Generalized Quadrangle

For a generalized quadrangle, the probability that any pair of blocks share a key is equal to the number of lines over the number of blocks:

$$P_{GQ} = \frac{t(s+1)}{b} = \frac{t(s+1)}{(t+1)(st+1)}.$$

This will always be **less than 1** when t is greater than 0.

The symmetric design has a higher probability of key-share.

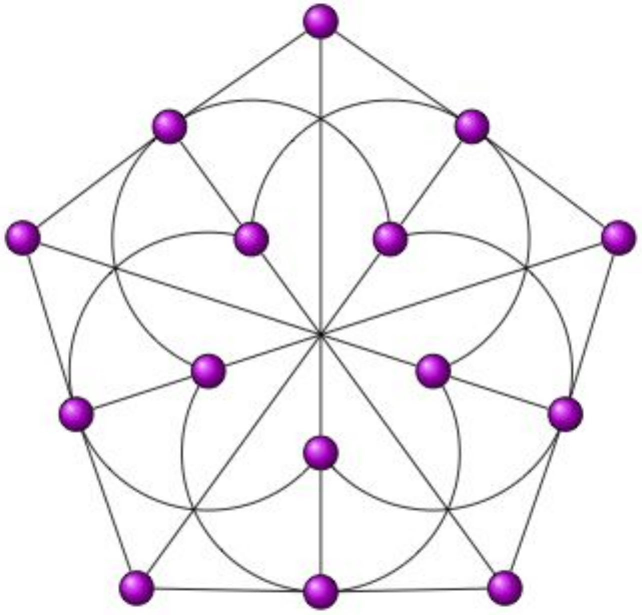
Generalized Quadrangle

With a GQ(s, t):

- Each point is a key
- Each line is a key-chain

Properties:

- Each line has $s+1$ points
- Each point has $t+1$ lines going through it
- GQ(s,t) has $v = (s+t)(st+1)$ points and $b = (t+1)(st+1)$ lines
- The construction runtime is $O(v^2)$



GQ(2,2)
Key-pool size: 15
Nodes/key-chains: 15

Performance

Metric	Most Optimized Design
Maximize number of blocks given block size	GQ(q, q^2)
Minimize block size given number of blocks	GQ(q^2, q^3)
Maximize resilience	GQ(q^2, q^3)
Maximize probability two blocks have a shared key	Symmetric Design
Maximize simplicity for construction	Symmetric Design