Covering Extended Building Sets…. Revisited

Jim Davis
University of Richmond
Singapore, May 24, 2016

Motivation

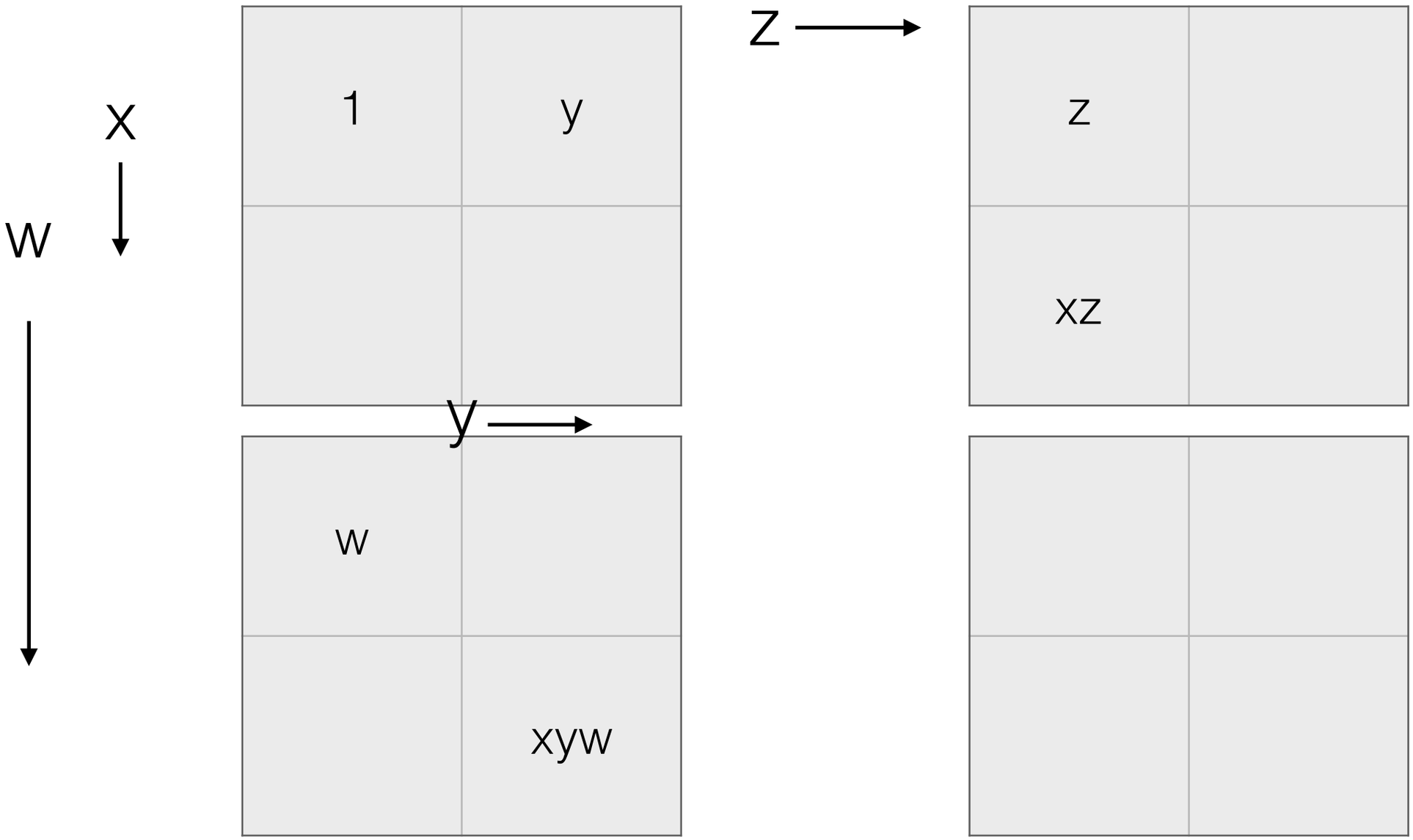
Motivation

99,270,589,265,934,370,305,785,861,242,880

Outline

- Refresher on Difference Sets
- Very brief overview of Character Theory
- Definition of Covering Extended Building Set
- Application to Bent functions
- Signatures, new constructions

Working example of a difference set



Working example of a difference set

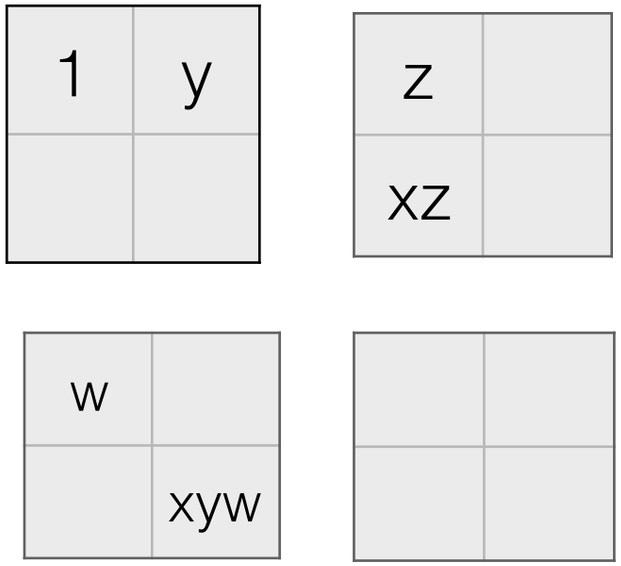
1	y

z	
xz	

w	
	xyw

D = {1,y,z,xz,w,xyw}

Working example of a difference set



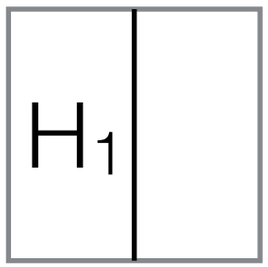
D = {1,y,z,xz,w,xyw}

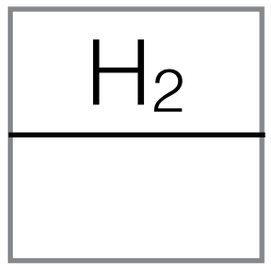
=<y> U z <x> U w <xy>

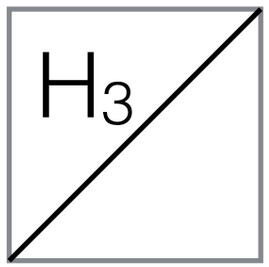
Character Theory

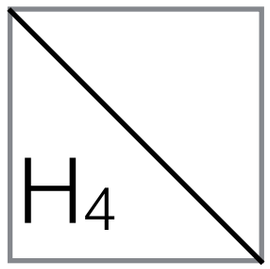
$$\chi(D) = \sqrt{n}$$

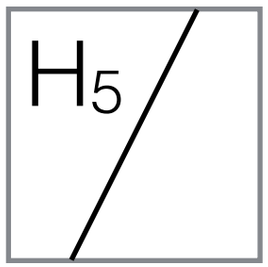
Hyperplanes

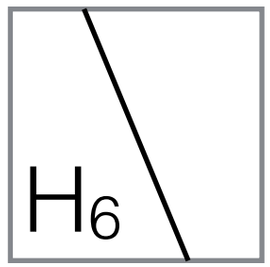


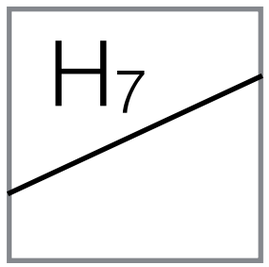


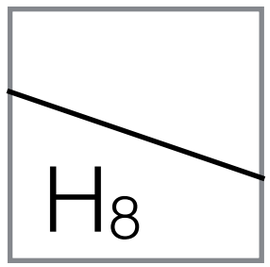




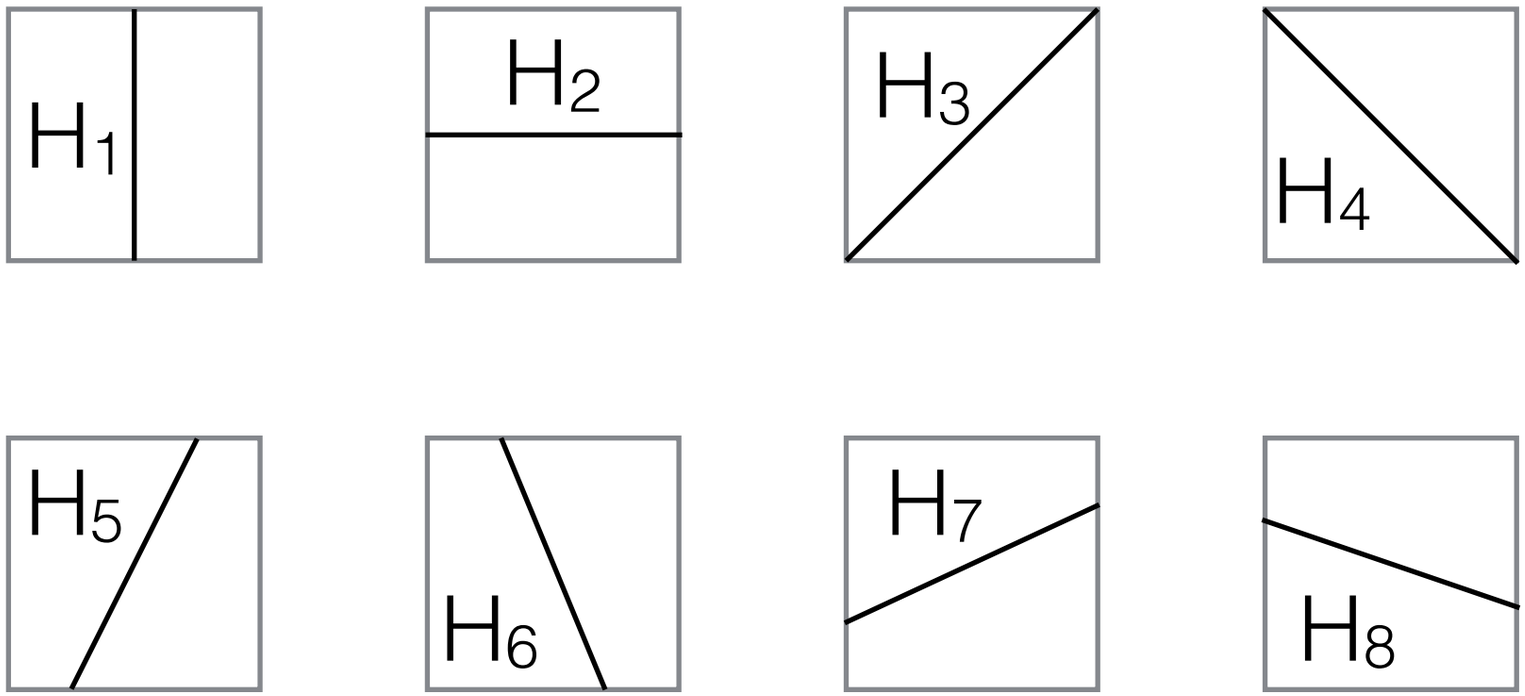








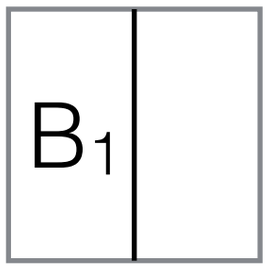
Hyperplanes

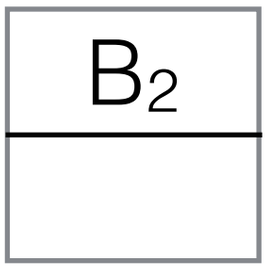


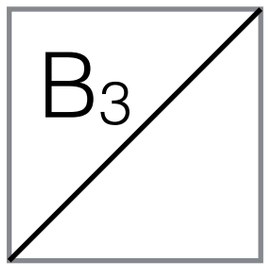
$$\chi(H_i) = 0, \chi(H_j) = |H_j|$$

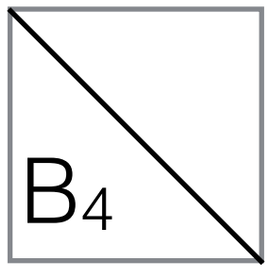
$$D = U g_i H_i$$

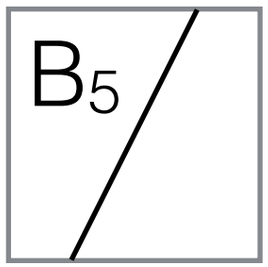
Covering EBS

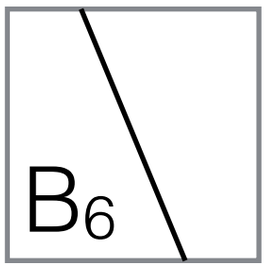


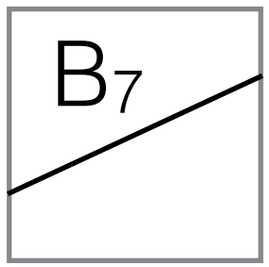


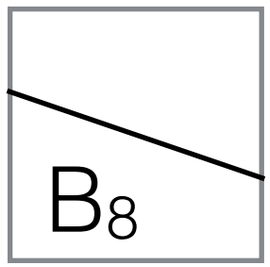












$$\chi(B_i) = 0, \chi(B_j) = |B_j|$$

$$D = U g_i B_i$$

99,270,589,265,934,370,305,785,861,242,880
8-variable bent functions

Equivalent to (256,120,56) difference sets in Z_2^8

99,270,589,265,934,370,305,785,861,242,880
8-variable bent functions

Equivalent to (256,120,56) difference sets in Z_2^8

Use a (32,8,4,-)-Cov EBS

Signatures

Blocks inside <x,y,z,w,u,v>:

x->1, y->1:

B1=<x,y,z> U u<x,y,w> U v<x,y,zw>

Signatures

Blocks inside <x,y,z,w,u,v>:

x->1, y->1:

B1=<x,y,z> U u<x,y,w> U v<x,y,zw>

x->1, y->-1:

B2=<x,z,w> U u<x,yz,w> U v<x,z,yw> U uv<x,yz,yw>

Signatures

Blocks inside <x,y,z,w,u,v>:

x->1, y->1:

B_1=<x,y,z> U u<x,y,w> U v<x,y,zw>

x->1, y->-1:

B_2=<x,z,w> U u<x,yz,w> U v<x,z,yw> U uv<x,yz,yw>

x->-1, y->1:

B_3=<y,z,w> U u<y,xz,w> U v<y,z,xw> U uv<y,xz,xw>

x->-1, y->-1:

B_4=<xy,z,w> U u<xy,yz,w> U v<xy,z,yw> U uv<xy,yz,yw>

$$D = B_1 \cup s\, B_2 \cup t\, B_3 \cup st\, B_4$$

Signatures (#2)

Blocks inside <x,y,z,w,u,v>:

x->1, y->1:

B_1=<x,y,z> U u<x,y,w> U v<x,y,zw>

x->1, y->-1:

B_2=<x,z,w> U u<x,yz,w> U v<x,z,yw> U uv<x,yz,yw>

x->-1, z->1:

B_5=<z,y,w> U u<z,xy,w> U v<z,y,xw> U uv<z,xy,xw>

x->-1, z->-1:

B_6=<xz,y,w> U u<xz,xy,w> U v<xy,y,xw> U uv<xy,xy,xw>

$$D = B_1 \cup s\, B_2 \cup t\, B_5 \cup st\, B_6$$

Signatures (#3)

Blocks inside <x,y,z,w,u,v>:

x->1, y->1:

B_1=<x,y,z> U u<x,y,w> U v<x,y,zw>

x->-1, z->1:

B_5=<z,y,w> U u<z,xy,w> U v<z,y,xw> U uv<z,xy,xw>

y->-1, z->-1:

B_7=<yz,x,w> U u<yz,xz,w> U v<yz,x,zw> U uv<yz,xz,zw>

xz->1, xy->-1:

B_8=<xz,x,w> U u<xz,y,w> U v<xz,x,xyw> U uv<xz,y,xyw>

$$D = B_1 \cup s\, B_5 \cup t\, B_7 \cup st\, B_8$$

Signatures (#3)

Blocks inside <x,y,z,w,u,v>:

x->1, y->1:

B_1=<x,y,z> U u<x,y,w> U v<x,y,zw>

x->-1, z->1:

B_5=<z,y,w> U u<z,xy,w> U v<z,y,xw> U uv<z,xy,xw>

y->-1, z->-1:

B_7=<yz,x,w> U u<yz,xz,w> U v<yz,x,zw> U uv<yz,xz,zw>

xz->1, xy->-1:

B_8=<xz,x,w> U u<xz,y,w> U v<xz,x,xyw> U uv<xz,y,xyw>

Constructs NEW BENT FUNCTIONS!

Signatures

Blocks inside <x,y,z,w,u,v>:

x->1, y->1:

B_1=<x,y,z> U u<x,y,w> U v<x,y,zw>

x->1, y->-1:

B_2=<x,z,w> U u<x,yz,w> U v<x,z,yw> U uv<x,yz,yw>

x->-1, y->1:

B_3=<y,z,w> U u<y,xz,w> U v<y,z,xw> U uv<y,xz,xw>

x->-1, y->-1:

B_4=<xy,z,w> U u<xy,yz,w> U v<xy,z,yw> U uv<xy,yz,yw>

Signatures

Blocks inside <x,y,z,w,u,v>:

x->1, y->1:

B_1=<x,y,z> U u<x,y,w> U v<x,y,zw>

x->1, y->-1:

B_2=<x,z,w> U z<x,yu,v> U w<x,u,yv> U zw<x,yu,yv>

x->-1, y->1:

B_3=<y,z,w> U u<y,xz,w> U v<y,z,xw> U uv<y,xz,xw>

x->-1, y->-1:

B_4=<xy,z,w> U u<xy,yz,w> U v<xy,z,yw> U uv<xy,yz,yw>

Subgroup for B_2:<x,y,u,v>

Signatures

Blocks inside <x,y,z,w,u,v>:

x->1, y->1:

B_1=<x,y,z> U u<x,y,w> U v<x,y,zw>

x->1, y->-1:

B_2=<x,z,w> U z<x,yu,v> U w<x,u,yv> U zw<x,yu,yv>

x->-1, y->1:

B_3=<y,zu,wv> U u<y,xzu,wv> U v<y,zu,xwv> U uv<y,xzu,xwv>

x->-1, y->-1:

B_4=<xy,zuv,w> U u<xy,yzuv,w> U v<xy,zuv,yw> U uv<xy,yzuv,yw>

Subgroup for B_2:<x,y,u,v>

Subgroup for B_3:<x,y,zu,wv>

Subgroup for B_4:<x,y,zuv,w>

Further work

- Determine how many bent functions constructible by Cov EBS
- Find other Cov EBSs that are not signature schemes
- Generalize to higher orders