# Open cases for cyclic difference sets : application of weil numbers

Tan, Ming Ming

2008

Tan, M. M. (2008, March). Open cases for cyclic difference sets- application of weil numbers. Presented at Discover URECA @ NTU poster exhibition and competition, Nanyang Technological University, Singapore.

https://hdl.handle.net/10356/95409

NANYANG TECHNOLOGICAL UNIVERSITY

**URECA** *Undergraduate Research Experience on CAmpus*

**Category: 6**
**Project ID: SPMS07075**

# Open Cases For Cyclic Difference Sets

# - Application Of Weil Numbers

## OVERVIEW

The study of cyclic difference sets is important in the field of design and coding theory.

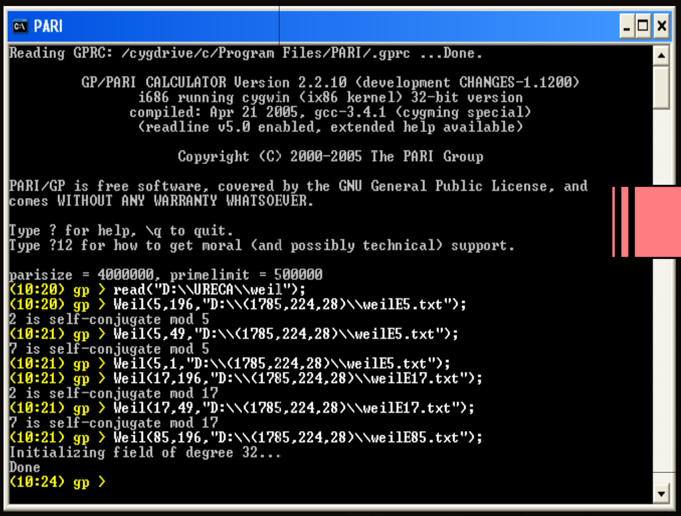
Many different approaches have been used to prove the existence or nonexistence of a cyclic difference set.

Still, there are some open cases in which the existence of a cyclic difference set is unknown.

## OBJECTIVE

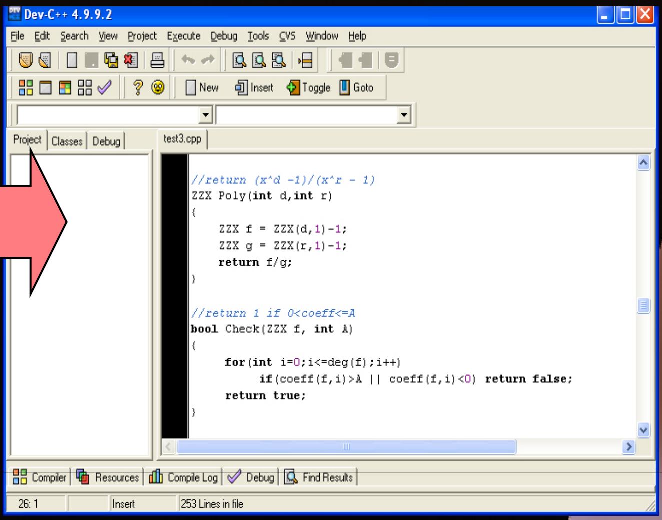
Tackle the list of open difference set parameters (source: La Jolla Difference Set Repository) with the application of weil numbers.

## METHODOLOGY



```
Reading GPRC: /cygdrive/c/Program Files/PARI/.gprc ...Done.

           GP/PARI CALCULATOR Version 2.2.10 (development CHANGES-1.1200)
                  i686 running cygwin (ix86 kernel) 32-bit version
                 compiled: Apr 21 2005, gcc-3.4.1 (cygming special)
                  (readline v5.0 enabled, extended help available)

                     Copyright (C) 2000-2005 The PARI Group

PARI/GP is free software, covered by the GNU General Public License, and
comes WITHOUT ANY WARRANTY WHATSOEVER.

Type ? for help, \q to quit.
Type ?12 for how to get moral (and possibly technical) support.

parisize = 4000000, primelimit = 500000
(10:20) gp > read("D:\\URECA\\weil");
(10:20) gp > Weil(5,196,"D:\\(1785,224,28)\\weilE5.txt");
2 is self-conjugate mod 5
(10:21) gp > Weil(5,49,"D:\\(1785,224,28)\\weilE5.txt");
7 is self-conjugate mod 5
(10:21) gp > Weil(5,1,"D:\\(1785,224,28)\\weilE5.txt");
(10:21) gp > Weil(17,196,"D:\\(1785,224,28)\\weilE17.txt");
2 is self-conjugate mod 17
(10:21) gp > Weil(17,49,"D:\\(1785,224,28)\\weilE17.txt");
7 is self-conjugate mod 17
(10:21) gp > Weil(85,196,"D:\\(1785,224,28)\\weilE85.txt");
Initializing field of degree 32...
Done
(10:24) gp >
```

Use of Weil Number Program



```
//return (x^d -1)/(x^r - 1)
ZZX Poly(int d,int r)
{
    ZZX f = ZZX(d,1)-1;
    ZZX g = ZZX(r,1)-1;
    return f/g;
}

//return 1 if 0<coeff<=A
bool Check(ZZX f, int A)
{
     for(int i=0;i<=deg(f);i++)
          if(coeff(f,i)>A || coeff(f,i)<0) return false;
     return true;
}
```

C++ Program for Various Computation

Computations:

- Generate all $D_d$ from the output of Weil Number Program:

$$D_d D_d^{-1} \equiv n \pmod{\Phi_d}$$

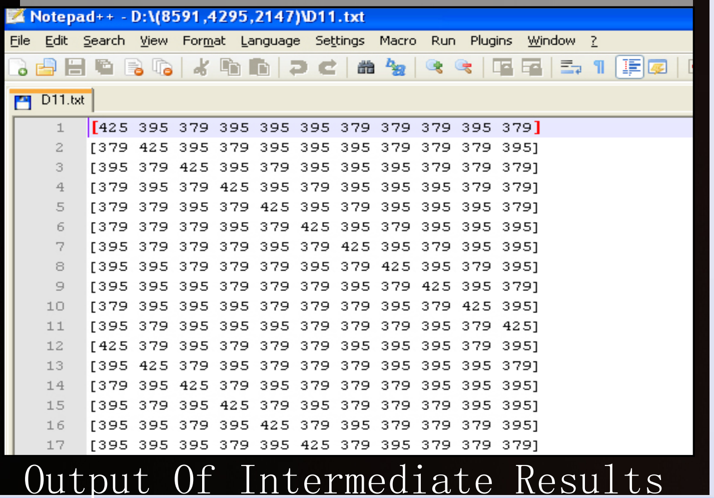
- Apply recursive formula:

$$dD_{[d]} \equiv dD_d - \sum_{\substack{r|d \\ r\neq d}} \mu\left(\frac{d}{r}\right) r\left(D_{[r]} - D_d\right)\left(\frac{x^d-1}{x^r-1}\right) \bmod\left(x^d-1\right)$$

to obtain

$$D_{[d]} \equiv \sum_{r=0}^{d-1} A_{r,d} x^r \pmod{x^d-1}$$

$$A_{r,d} \leq 0,\ A_{r,d} \leq \frac{v}{d},\ A_{r,d} \in Z$$


Notepad++ - D:\(8591,4295,2147)\D11.txt
File Edit Search View Format Language Settings Macro Run Plugins Window ?
D11.txt

```
[425 395 379 395 395 395 379 379 379 395 379]
[379 425 395 379 395 395 395 379 379 379 395]
[395 379 425 395 379 395 395 395 379 379 379]
[379 395 379 425 395 379 395 395 395 379 379]
[379 379 395 379 425 395 379 395 395 395 379]
[379 379 379 395 379 425 395 379 395 395 395]
[395 379 379 379 395 379 425 395 379 395 395]
[395 395 379 379 379 395 379 425 395 379 395]
[395 395 395 379 379 379 395 379 425 395 379]
[379 395 395 395 379 379 379 395 379 425 395]
[395 379 395 395 395 379 379 379 395 379 425]
[425 379 395 379 379 379 395 395 395 379 395]
[395 425 379 395 379 379 379 395 395 395 379]
[379 395 425 379 395 379 379 379 395 395 395]
[395 379 395 425 379 395 379 379 379 395 395]
[395 395 379 395 425 379 395 379 379 379 395]
[395 395 395 379 395 425 379 395 379 379 379]
```

Output Of Intermediate Results

## RESULTS

Following open cases are solved:

(1)(1785,224,28)

(2)(639,232,84)

(3)(5859,203,7)

(4)(8591,4295,2147)

## FUTURE PLAN

Solve the remaining open cases

**School of Physical and Mathematical Sciences**
**Project Title: Application of Number Theoretic Methods to Problems in Design and Coding Theory**
**Student: Tan Ming Ming**
**Supervisor: A/P Bernhard Schmidt**