Last time:

Thm: If $q = 4n-1$ prime power, $QR(q)$ is a $(4n-1, 2n-1, n-1)$-difference set.

We showed: (Lemma) $x \in QR(q) \iff -x \notin QR(q)$ (assuming $x \neq 0$)

In particular, there are $\frac{q-1}{2}$ quadratic residues ($= 2n-1$).

So, it remains to show that $\lambda = n-1$ for this (alleged) difference set.

Proof (thm)

We need to show that this satisfies the definition of a difference set, i.e. For every $x \in GF(q)^\times$, there are $n-1$ ways to write $x = r - s$, $r, s \in QR(q)$.

Equivalently, we must show that there are $(4n-1)$ ways to write $x = a^2 - b^2$ $(a, b \in GF(q)^\times)$.

$\iff x = (a-b)(a+b)$

↑ The reason of 4 comes in since a^2, b^2 have 2 square root each.

Claim: $x = a^2 - b^2 \iff a = \frac{c + c^{-1}x}{2}$, $b = \frac{c^{-1}x - c}{2}$, where $c \neq 0$

Proof:

($\Rightarrow$) Suppose $x = (a-b)(a+b)$. Put $c = a-b$. Since $x \neq 0$, then $c \neq 0$. Now solve for a, b in terms of x

$$\frac{x}{c} = a+b \quad \Rightarrow \quad \frac{x}{c} + c = 2a$$

$$c = a-b \qquad \frac{x}{c} - c = 2b$$

$\Leftarrow$

Proof (thm) (cont)

Proof (claim) (cont)

($\Leftarrow$) Check that

$$\left(\frac{c+c^{-1}x}{2}\right)^2 - \left(\frac{c^{-1}x-c}{2}\right)^2 = x.$$

□

But, we haven't checked that $a, b \neq 0$.

Claim: $ab \neq 0 \Leftrightarrow c^2 \neq \pm x$.

Proof:

If $c^2 = x$, then $b = 0$ and if $c^2 = -x$, then $a = 0$

(Plug x into the formulas for a, b.)

If neither, then neither $a, b = 0$. □

Combining claims (1) and (2), the # pairs $(a,b) \in (\mathbb{F}_q)^{\times 2}$ s.t. $x = a^2 - b$ $(a,b \neq 0)$ is the # of $c \in \mathbb{F}(q)$ s.t. $c \neq 0$ and $c^2 \neq \pm x$.

Finally, by the lemma, either $x \in \mathbb{F}(q)$ or $-x \in \mathbb{F}(q)$, but not both.

If $x \in \mathbb{F}(q)$, there are 2 values of c, s.t. $c^2 = x$ and no values of c such that $c^2 = -x$.

If $-x \in \mathbb{F}(q)$, other way around.

↪

Proof: (cont.)

Either way, those are 3 values of c that don't work, therefore the # of solutions is $q-3 := (n-1)$ from "good c's". ✱

In particular, this is the same for every value of $x \in QR(q)^*$.

So, it's a difference set ∎

Remark:

If $q \equiv 1 \pmod 4$, then the last part of the argument breaks down. Since

$$x \in QR(q) \iff -x \in QR(q)$$

and so there are 5 forbidden values of c (including $c=0$)

And further, if $x \notin QR(q)$ (so $-x \notin QR(q)$), then there is only 1 forbidden value of c (c that is $c=0$).

So, we definitely don't get a ~~different~~ difference set in general if $q \equiv 1 \pmod 4$.

BUT, we can do something slightly different -

Conference Matrices:

Defn: An $n \times n$ matrix C is a conference matrix if $c_{ii} = 0$, $c_{ij} \in \{1, -1\}$ for $i \neq j$ and $CC^T = (n-1)I_n$.

↑ Dot product of any row w itself.

Note: As with Hadamard matrices, the condition $CC^T = (n-1)I_n$ $\Rightarrow C^TC = (n-1)I_n$

Example:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Symmetric

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & -1 & 1 \\ -1 & 1 & 0 & -1 \\ -1 & -1 & 1 & 0 \end{pmatrix}$$

Skew Symmetric.

Monomial Equivalence:

If C is a conference matrix, H_1, H_2 monomial matrices

[If $H_1 C H_2$ has 0's on the diagonal then it's a conference matrix.

(If we think about this for a bit, this condition is true $\Leftrightarrow$ $H_1 H_2$ is a diagonal matrix)