Applications of Weil's Theorem on Character Sums

Tony Forbes ADF32A version 1.9A

Notes for a talk given at LSBU on 7 September 2007

Finite fields

$\mathbb{F}_q$ is the finite field of q elements, q a power of a prime p. $\mathbb{F}_q$ is the splitting field of $X^q - X$ over $\mathbb{F}_p$. $\mathbb{F}_q$ is unique up to isomorphism.

Let $r = q^k$. Every automorphism of $\mathbb{F}_r$ over $\mathbb{F}_q$ is of the form $x \mapsto x^{qi}, i = 0, 1, \ldots, k-1$. Thus the Galois group of $\mathbb{F}_r$ over $\mathbb{F}_q$ is cyclic with generator $x \mapsto x^q$.

The *trace* of an element $x \in \mathbb{F}_r$ is $\mathcal{T}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{k-1}}$.

Differential operator: $D(a_0 + a_1x + \cdots + a_nx^n) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$. Suppose $\mathbb{K}$ is a field of characteristic p, $m \le p$, $a(x)$ is a polynomial in $\mathbb{K}[x]$, and for some $x_0 \in \mathbb{K}$,

$$a(x_0) = Da(x_0) = D^2a(x_0) = \cdots = D^{m-1}a(x_0) = 0.$$

Then $a(x)$ has a zero of order m at x_0. Thus $(x - x_0)^m | a(x)$. The condition $m \le p$ is essential.

Multiplicative characters

A multiplicative *character* χ is a homomorphism from $\mathbb{F}_q^*$ the multiplicative group of $\mathbb{F}_q$ into the complex unit circle. We extend the homomorphism to a map from the whole field by setting $\chi(0) = 0$. We have

$$\chi(1) = 1;$$
$$\chi(xy) = \chi(x)\chi(y).$$

If χ_1 and χ_2 are characters, then so is $\chi_1\chi_2$. If χ is a character, then so is $1/\chi$. The characters form a group under multiplication; the identity element is the *trivial character* χ_0 defined by

$$\chi_0(x) = 1 \text{ for } x \ne 0, \qquad \chi_0(0) = 0.$$

The *order* of a character χ is the smallest non-zero d such that $\chi^d = \chi_0$.

$$\sum_{x \in \mathbb{F}_q} \chi(x) \;=\; \begin{cases} q-1 & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise.} \end{cases}$$

$$\sum_{\chi} \chi(x) \;=\; \begin{cases} q-1 & \text{if } x = 1, \\ 0 & \text{otherwise.} \end{cases}$$

A concrete construction

The multiplicative group of $\mathbb{F}_q$ is cyclic of order $q-1$. Let ω be a generator; ω is usually called a *primitive element* of $\mathbb{F}_q$, or, if q is prime, a *primitive root* of q. Define $\log_\omega x$ by $n = \log_\omega x$ iff $x = \omega^n$. (I used to write ind but nowadays log seems to be fashionable.)

For $a = 0, 1, \ldots, q-2$, define χ_a by

$$\chi_a(x) \;=\; \exp\left(2\pi i \,\frac{a \log_\omega x}{q-1}\right), \; x \ne 0, \qquad \chi_a(0) = 0.$$

Note that exp is the usual exponential function and that you can't cancel exp and log. Trivial character: $a = 0$. Quadratic character: $a = (q-1)/2$. The order of χ_a is the smallest non-zero d for which $\chi_a(\omega^d) = 1$; this is $(q-1)/\gcd(a, q-1)$.

WEIL'S THEOREM

Theorem 1 (Weil, 1940, 1948; [5, page 43]) *Suppose χ is a multiplicative character of order $d > 1$ in $\mathbb{F}_q$. Suppose $f(x) \in \mathbb{F}_q[x]$ is a polynomial whose set of zeros in its splitting field over $\mathbb{F}_q$ has cardinality m, and suppose $f(x)$ is not a constant multiple of a d-th power. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \ \leq \ (m-1)\sqrt{q}.$$

Roughly speaking, we count solutions of the hyperelliptic equation $f(x) = y^d$, where $f(x)$ is a polynomial of degree m. The main result is that under certain conditions there are $q \pm$ (something small) solutions (x, y) of $f(x) = y^d$ over $\mathbb{F}_q$.

In the following, absolutely irreducible means irreducible in $\mathbb{F}_q$ and every algebraic extension of $\mathbb{F}_q$. Algebraic means each element is a zero of a polynomial (i.e. not transcendental).

Weil, 1940, used algebraic geometry to prove the following.

Theorem 2 *Let $F(x, y)$ be an absolutely irreducible polynomial of total degree t with coefficients in $\mathbb{F}_q$ and N zeros (x, y), $x, y \in \mathbb{F}_q$. Then*

$$|N - q| \leq 2g\sqrt{q} + O_t(1),$$

where g is the genus of the curve $F(x, y) = 0$.

This is the Riemann Hypothesis for curves over finite fields. Since $g \leq \binom{t-1}{2}$,

$$|N - q| \leq (t-1)(t-2)\sqrt{q} + O_t(1).$$

Henceforth consider only the special case $F(x, y) = y^d - f(x)$, where $f(x)$ has degree m.

The cases $d = 2, m = 3, 4$ for $q = p$ prime were conjectured by Artin, 1924, in the form

$$|N - q| \leq 2\sqrt{p}, \quad m = 3; \qquad |N + 1 - q| \leq 2\sqrt{p}, \quad m = 4,$$

and proved by Hasse in 1936 for prime power q. Using elementary methods Stepanov, 1969, 1970, 1971, 1972, 1974, proved

$$|N - q| = O_d(\sqrt{q}).$$

There is an elementary proof of Weil's theorem in [5, pages 1–80].

How to get from counting solutions to character sums

Theorem 3 ([5, page 10], Stepanov) *Suppose $f(x) - y^d$ is absolutely irreducible and that $q > 100dm^2$, where m is the degree of $f(x)$. Let N be the number of zeros of $f(x) - y^d$. Then*

$$|N - q| \ \leq \ 4md^{3/2}\sqrt{q}.$$

Absolute irreducibility is vital. See Examples 1 and 2 in [5, pages 9–10].

Example 1. $y^2 = x^4 + 2x^2 + 1$. Factorize: $(y - (x^2+1))(y + (x^2+1)) = 0$. Then either $y = x^2 + 1$ or $y = -(x^2 + 1)$. Hence $\approx 2q$ solutions. But $y^2 - f(x)$ is reducible over $\mathbb{F}_q$.

Example 2. Consider $y^2 = 2x^4 + 4x^2 + 2$ over $\mathbb{F}_p$, $p \equiv 5 \pmod 8$. Factorize: $(y - \sqrt{2}(x^2 + 1))(y + \sqrt{2}(x^2+1)) = 0$. But not in $\mathbb{F}_p$ since $\sqrt{2}$ does not exist in $\mathbb{F}_p$. But $x^2 - 2$ is irreducible over $\mathbb{F}_p$. Hence $\sqrt{2}$ exists in $\mathbb{F}_{p^2}$ and the factorization is valid. Thus $2x^4 + 4x^2 + 2 - y^2$ is irreducible but not absolutely irreducible over $\mathbb{F}_p$. Moreover $y^2 = 2x^4 + 4x^2 + 2$ has no solutions in $\mathbb{F}_p$.

In both cases the conclusion of Theorem 3 is false.

Theorem 4 [5, page 92]) *Let*

$$F(x,y) = y^d + g_1(x)y^{d-1} + \cdots + g_d(x), \qquad \psi(F) = \max_{1\le i\le d} \frac{\deg g_i}{i}.$$

Suppose that $\psi(F) = \dfrac{n}{d}$ *for some* n *coprime to* d. *Then* $F(x,y)$ *is absolutely irreducible.*

So, for example, $y^2 -$ (any cubic in x) is absolutely irreducible.

Lemma 1 *Let* ω *be a primitive element of* $\mathbb{F}_q$ *and suppose* $\chi \neq \chi_0$ *is a character such that* $\chi^d = \chi_0$ *for some* $d > 1$. *Then*

$$\sum_{k=0}^{d-1} \chi(\omega^k) = 0.$$

Proof. This is obvious. □

Theorem 5 [5, page 42] *Suppose* $d|q-1$ *and suppose* $\chi \neq \chi_0$ *is a character of order* d. *Suppose* $f(x) \in \mathbb{F}_q[x]$ *is a polynomial of degree* m. *Suppose* $f(x) - y^d$ *is absolutely irreducible. Then if* $q > 100dm^2$,

$$\left|\sum_{x\in\mathbb{F}_q} \chi(f(x))\right| \;<\; 5md^{3/2}\sqrt{q}.$$

Proof [5, page 50]. Let ω be a primitive element of $\mathbb{F}_q$. Let Z_k denote the number of x such that $f(x) = \omega^{k+ad}$ for some a. Then

$$\sum_{x\in\mathbb{F}_q} \chi(f(x)) = \sum_{k=0}^{d-1} Z_k \chi(\omega^k).$$

Let N_k denote the number of (x,y) such that

$$y^d = f(x)\omega^{-k}.$$

Furthermore $y^d - f(x)\omega^{-k}$ is absolutely irreducible (not too difficult to prove: see [5, Lemma 2C, pages 11–12]). So we use Theorem 3 to get

$$|N_k - q| < 4md^{3/2}\sqrt{q}.$$

Let N_k' be the number of solutions of $y^d = f(x)\omega^{-k}$ with $y \neq 0$. Then $|N_k' - N_k| \le m$. So

$$|N_k' - q| < 5md^{3/2}\sqrt{q}.$$

But $Z_k = N_k'/d$ (think about it) and if we write $Z_k = q/d + R_k$, then

$$|R_k| < 5md^{1/2}\sqrt{q}.$$

Thus, using Lemma 1,

$$\left|\sum_{x\in\mathbb{F}_q} \chi(f(x))\right| = \left|\sum_{k=0}^{d-1} \left(\frac{q}{d} + R_k\right)\chi(\omega^k)\right| = \left|\sum_{k=0}^{d-1} R_k\chi(\omega^k)\right| \le \sum_{k=0}^{d-1} |R_k| = 5md^{3/2}\sqrt{q}. \quad \square$$

PALEY GRAPHS

Paley graph: Vertices are elements in $\mathbb{F}_q$, where $q \equiv 1 \pmod 4$ is a prime power. An edge $x \sim y$ exists iff $x-y$ is a (non-zero) square. It is an SRG$(q,(q-1)/2,(q-5)/4,(q-1)/4)$. Paley graphs with $q \geq 29$ are 3-e-c (Ananchuen & Caccetta, 1993).

Paley graphs are n-e-c whenever $q > n^2 2^{2n-2}$ (Bollobás & Thomason, 1981; Blass, Rossman & Harary, 2005).

Theorem 6 *Given $n \geq 1$, the Paley graph on $\mathbb{F}_q$ is n-e-c for all sufficiently large prime powers $q \equiv 1 \pmod 4$.*

Proof. Assume $n \geq 1$ is fixed. Given sets J, K of elements of $\mathbb{F}_q$ such that $J \cap K = \emptyset$ and $|J \cup K| = n$, we prove that for sufficiently large q there is an x such that $x - j$ is a non-zero square for all $j \in J$ and $x - k$ is not a square for all $k \in K$. Such an x is said to be *correctly connected to J and K*.

Let θ be the quadratic character. Let

$$\pi(x) = \prod_{j \in J}(1 + \theta(x-j)) \prod_{k \in K}(1 - \theta(x-k)).$$

If x is correctly connected to J and K, then $\pi(x) = 2^n$. If x is not correctly connected to J and K, then $\pi(x) = 0$ except possibly for at most n values of x where $\pi(x) \leq 2^{n-1}$. Let $\Delta = \sum_{x \in \mathrm{GF}(q)} \pi(x)$. If there is no x correctly connected to J and K, then $\Delta \leq n2^{n-1}$. Now

$$\begin{aligned}
\Delta &= \sum_{x \in \mathbb{F}_q} \sum_{R \subseteq J, S \subseteq K} (-1)^{|S|} \prod_{j \in R} \theta(x-j) \prod_{k \in S} \theta(x-k) \\
&= q + \sum_{x \in \mathbb{F}_q} \sum_{R \subseteq J, S \subseteq K, |R \cup S| > 0} (-1)^{|S|} \prod_{j \in R} \theta(x-j) \prod_{k \in S} \theta(x-k) \\
&= q + O\left(\sum_{R,S} \sum_{x \in \mathbb{F}_q} \theta\left(\prod_{j \in R}(x-j) \prod_{k \in S}(x-k) \right) \right) \\
&= q + O\left(\sum_{R,S} \sqrt{q} \right) \;=\; q + O(\sqrt{q}),
\end{aligned}$$

which is greater than $n2^{n-1}$ for sufficiently large q. □

SIX-SPARSE STEINER TRIPLE SYSTEMS $v \equiv 7 \pmod{12}$ [3]

Block transitive Steiner triple systems with $v \equiv 7 \pmod{12}$, v prime

Let ω be a primitive root mod v. Let χ be the character defined by $\chi(x) = \exp(2\pi i \log_\omega x/6)$, and $\chi(0) = 0$. Observe that $6|v-1$. The order of χ is 6.

We want to define a block transitive STS(v) generated by $\{0, 1, \alpha\}$ under the action of maps $x \mapsto \tau x + m$, where $\tau, m \in \mathbb{F}_v$ and $\chi(\tau) = 1$; i.e. τ is a 6th power.

For this to work, the six differences in $\tau\{0,1,\alpha\}$, i.e $\pm\tau$, $\pm\tau\alpha$, $\pm\tau(1-\alpha)$, must be distinct whenever $\chi(\tau) = 1$. In other words, the 'logarithms' of ± 1, $\pm\alpha$ and $\pm(1-\alpha)$ must be distinct modulo 6. Since $v \equiv 3 \pmod 4$, $\log(-1) \equiv 3 \pmod 6$. So $\chi(\alpha) \neq 0, \pm 1$ and $\chi(\alpha)\chi(1-\alpha) = \pm 1$. We also need $\chi(-1) = -1$; hence $v \equiv 1 \pmod{12}$ won't work. One possibility:

$\log_\omega \alpha \pmod 6$	0	1	2	3	4	5
	1	α	$(1-\alpha)$	-1	$-\alpha$	$-(1-\alpha)$

Example: $v = 19$, $\omega = 2$, $\omega^6 = 7$.

x	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_2 x$	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

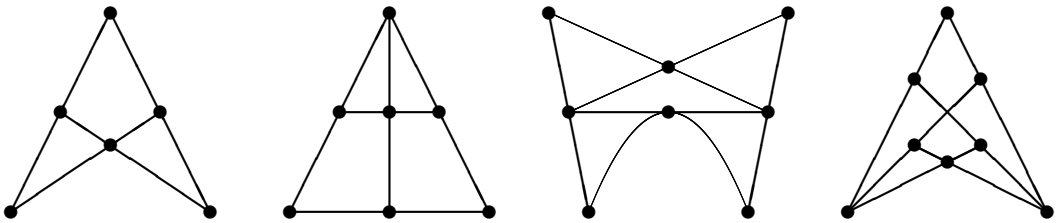
$\chi(x) = \exp(\pi i \log_2(x)/3)$, $\alpha = 4$, $(1 - \alpha) = 16$.

$\log \alpha = 2$, $\log -\alpha = 11$, $\log(1 - \alpha) = 4$, $\log -(1 - \alpha) = 13$.

Hence the system generated by $\{0, 1, 4\}$ is a block transitive STS(19). It is a cyclic STS(19) with starter blocks got by multiplying by 7: $\{0, 1, 4\}$, $\{0, 7, 9\}$, $\{0, 11, 6\}$.

6-sparse Steiner triple systems

We were interested in 6-sparse STS(v)s, systems which avoid these configurations:



4-cycle (Pasch) mitre crown 6-cycle

And indeed we found 29 block transitive systems [3]:

v	α	v	α	v	α	v	α
139	51	907	68	1303	971	2707	1837
139	118	967	210	1531	42	3259	562
151	37	991	76	1699	506	3259	1286
463	261	1039	356	2083	800	3319	511
523	501	1051	660	2179	1820	4447	210
571	528	1087	519	2311	1593		
691	468	1171	931	2503	1287		
859	616	1291	833	2539	180		

Block transitive 6-sparse Steiner triple systems.

Search limit: 9,150,625; no more block transitive 6-sparse systems.

Lemma 2 *Suppose that v is prime and that χ is a multiplicative character of $\mathbb{F}_v$ of order $d \geq 2$. Suppose also that $f_1(x), f_2(x), \ldots, f_n(x)$ are linear polynomials over $\mathbb{F}_v$ with distinct roots. Then if v is sufficiently large, there exists $x \in \mathbb{F}_v$ such that*

$$\chi(f_1(x)) = \chi(f_2(x)) = \ldots = \chi(f_n(x)) = 1. \tag{1}$$

Proof. Observe first that the possible values of $\chi(x)$ are the d dth roots of unity when $x \neq 0$, and $\chi(0) = 0$. Put

$$\pi(x) = \left(\sum_{i_1=0}^{d-1} \chi(f_1(x)^{i_1})\right)\left(\sum_{i_2=0}^{d-1} \chi(f_2(x)^{i_2})\right)\ldots\left(\sum_{i_n=0}^{d-1} \chi(f_n(x)^{i_n})\right).$$

If (1) holds then $\pi(x) = d^n$. Otherwise $\pi(x) = 0$ except for a number of values of x that depends only on d and n. (Recall that $0^0 = 1$.)

Next put $\Delta = \sum_{x \in \mathbb{F}_v} \pi(x)$. Note that if we can prove that $\Delta \to \infty$ as $v \to \infty$ then it will follow that there exists an $x \in \mathbb{F}_v$ which satisfies (1). But $\pi(x)$ has the form

$$\pi(x) = 1 + \sum_{\substack{i_1,i_2,\ldots,i_n=0 \\ i_1+i_2+\ldots+i_n \neq 0}}^{d-1} \chi((f_1(x))^{i_1}(f_2(x))^{i_2}\ldots(f_n(x))^{i_n}).$$

So

$$\Delta = v + \sum_{\substack{i_1,i_2,\ldots,i_n=0 \\ i_1+i_2+\ldots+i_n \neq 0}}^{d-1} \sum_{x \in GF(v)} \chi((f_1(x))^{i_1}(f_2(x))^{i_2}\ldots(f_n(x))^{i_n}).$$

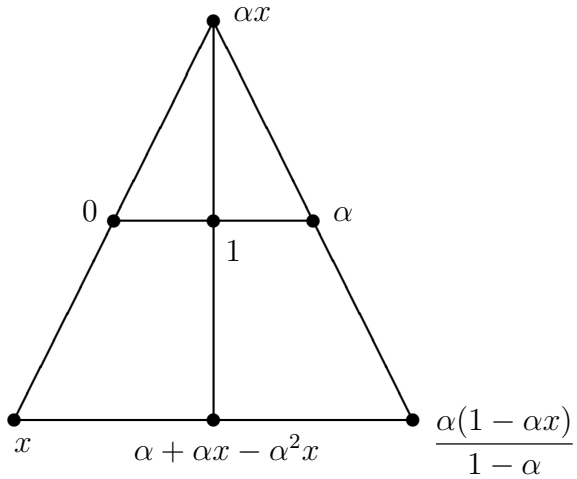
Since the $f_i(x)$ are linear polynomials in x with distinct roots, a product of the form $(f_1(x))^{i_1}(f_2(x))^{i_2}\ldots(f_n(x))^{i_n}$ with $0 \leq i_1, i_2, \ldots, i_n \leq d-1$ cannot be a constant multiple of a sixth power of a polynomial in x unless $i_1 = i_2 = \ldots = i_n = 0$. Hence, by Theorem 1 and provided that $i_1 + i_2 + \ldots + i_n \neq 0$, we have

$$\sum_{x \in \mathrm{GF}(v)} \chi((f_1(x))^{i_1}(f_2(x))^{i_2}\ldots(f_n(x))^{i_n}) = O(\sqrt{v}),$$

Hence

$$|\Delta| = v + O(\sqrt{v}). \qquad \square$$

We use Lemma 1 to show that the following mitre configuration is unavoidable for sufficiently large v.



Its blocks are

$$\begin{aligned}
&\{0, 1, \alpha\},\\
&\{0, x, \alpha x\} = x\{0, 1, \alpha\},\\
&\{\alpha x, 1, \alpha + \alpha x - \alpha^2 x\} = (1 - \alpha x)\{0, 1, \alpha\} + \alpha x,\\
&\left\{\frac{\alpha(1-\alpha x)}{1-\alpha}, \alpha x, \alpha\right\} = \left(\frac{\alpha(x-1)}{1-\alpha}\right)\{0, 1, \alpha\} + \frac{\alpha(1-\alpha x)}{1-\alpha},\\
&\left\{\frac{\alpha(1-\alpha x)}{1-\alpha}, x, \alpha + \alpha x - \alpha^2 x\right\} = \left(\frac{(\alpha^2-\alpha+1)x - \alpha}{1-\alpha}\right)\{0, 1, \alpha\} + \frac{\alpha(1-\alpha x)}{1-\alpha}.
\end{aligned}$$

These are five distinct blocks of S provided that x is selected to satisfy

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

Now apply Lemma 2 with $d = 6$, $n = 4$, $f_1(x) = x$, $f_2(x) = 1 - \alpha x$, $f_3(x) = \dfrac{\alpha(x-1)}{1-\alpha}$ and $f_4(x) = \dfrac{(\alpha^2 - \alpha + 1)x - \alpha}{1-\alpha}$.

With a more refined argument we can show that if $v > 9,150,625$, then an x with the desired property exists.

PERFECT STEINER TRIPLE SYSTEMS $v \equiv 7 \pmod{12}$

k-cycle configurations

Look at the pictures of the 4-cycle and the 6-cycle, above. Generalize to a k-cycle, k even.

Take a pair of points $\{a, b\}$ in a Steiner triple system of order v. Choose a point z not in the block defined by $\{a, b\}$. This defines two blocks, $\{a, z, c_1\}$ and $\{b, z, c_2\}$, say, and two more blocks, $\{a, c_2, d_1\}$, and $\{b, c_1, d_2 g\}$. (Draw a diagram!)

Now one of two things can happen: $d_1 = d_2$ or $d_1 \neq d_2$. If $d_1 = d_2$ we have a 4-cycle. If $d_1 \neq d_2$ we have two more blocks, $\{a, d_2, e_1\}$ and $\{b, d_1, e_2\}$, say.

If $e_1 = e_2$ we have a 6-cycle; otherwise we have two more blocks, $\{a, e_2, f_1\}$ and $\{b, e_1, f_2\}$.

We continue the process as far as possible. Eventually we will run out of points and the thing will stop in the manner described above with a k-cycle for some even k, $4 \leq k \leq v-3$. If for any pair $\{a, b\}$ this process always stops with a $(v-3)$-cycle, then the Steiner triple system is called *perfect*.

The cycle graph of a Steiner triple system

More formally, we define the *cycle graph*, $G_{a,b}$ for distinct points a and b of an STS(v). The vertices are the points of the STS(v) other than those in the block containing a and b. An edge $x \sim y$ occurs iff either $\{a, x, y\}$ or $\{b, x, y\}$ is a block.

By working through the process described above it is easy to see that $G_{a,b}$ is a union of disjoint cycles $C_{k_1} \cup C_{k_2} \cup \cdots \cup C_{k_r}$, where $r \geq 1$, k_i is even, $k_i \geq 4$, $i = 1, 2, \ldots, r$, and $k_1 + k_2 + \cdots + k_r = v - 3$. Moreover, if we take any one of the constituent cycle graphs, C_{k_i}, say, then the set of k_i blocks

$$\{\{a, x, y\} : \{x, y\} \text{ is an edge of } C_{k_i}\} \cup \{\{b, x, y\} : \{x, y\} \text{ is an edge of } C_{k_i}\}$$

is a k-cycle configuration. Thus k-cycle configurations are unavoidable in Steiner triple systems. In fact, for each pair of points a, b there will be a set of k-cycle configurations involving a total of $v - 3$ blocks.

Perfect Steiner triple systems

A Steiner triple system is perfect if every graph $G_{a,b}$ is a single cycle, C_{v-3}.

Perfect block transitive Steiner triple systems

v	7	79	139	367	811	1531	25771	50923	61339	69991	135859
α	3	29	25	112	18	84	4525	12999	630	7175	49142
k-sparse		5	6	5	5	4	4	4	4	4	4

As with block transitive 6-sparse systems, we can prove that there are only finitely many block transitive perfect Steiner triple systems.

In fact we prove that subject to certain conditions a particular 12-cycle is unavoidable in block transitive Steiner triple systems. The proof uses Weil's theorem.

The blocks of the 12-cycle are denoted by B_i for $i = 1, 2, \ldots, 12$, where $B_1 = \{0, z_1, z_2\}$, $B_2 = \{a, z_2, z_3\}$, $B_3 = \{0, z_3, z_4\}, \ldots,$ $B_{12} = \{a, z_{12}, z_1\}$. The point a and the twelve points z_i

are given in terms of a parameter x as follows.

$$a = (1-\alpha)x + \alpha, \quad z_1 = 1, \quad z_2 = \alpha, \quad z_3 = \alpha - \alpha x, \quad z_4 = 1 - x,$$
$$z_5 = \frac{2(1-\alpha)x}{\alpha} + \frac{2\alpha - 1}{\alpha}, \quad z_6 = -2x + \frac{2\alpha - 1}{\alpha - 1},$$
$$z_7 = -\frac{(\alpha+1)x}{\alpha - 1} + \frac{\alpha^2}{(\alpha-1)^2}, \quad z_8 = -\frac{\alpha(\alpha+1)x}{\alpha - 1} + \frac{\alpha^3}{(\alpha-1)^2},$$
$$z_9 = 2\alpha x - \frac{\alpha^2}{\alpha - 1}, \quad z_{10} = 2\alpha(1-\alpha)x + \alpha^2, \quad z_{11} = \alpha x, \quad z_{12} = x.$$

Each block B_i can be expressed as $\mu_i\{0, 1, \alpha\} + \nu_i$ where the values of μ_i are as follows.

$$\mu_1 = 1, \quad \mu_2 = x, \quad \mu_3 = 1 - x, \quad \mu_4 = \frac{(2-\alpha)x}{\alpha} + \frac{\alpha - 1}{\alpha},$$
$$\mu_5 = \frac{2x}{\alpha} + \frac{1 - 2\alpha}{\alpha(\alpha - 1)}, \quad \mu_6 = -\frac{(\alpha-3)x}{\alpha - 1} + \frac{\alpha^2 - 3\alpha + 1}{(\alpha-1)^2},$$
$$\mu_7 = -\frac{(\alpha+1)x}{\alpha - 1} + \frac{\alpha^2}{(\alpha-1)^2}, \quad \mu_8 = \frac{(3\alpha-1)x}{\alpha - 1} + \frac{\alpha - 2\alpha^2}{(\alpha-1)^2},$$
$$\mu_9 = -2\alpha x + \frac{\alpha^2}{\alpha - 1}, \quad \mu_{10} = (1-2\alpha)x + \alpha, \quad \mu_{11} = x, \quad \mu_{12} = 1 - x.$$

These 12 blocks form a 12-cycle provided that $\chi(\mu_i) = 1$ for each i and α satisfies one or two extra conditions. Use Lemma 2 with $d = 6$, $n = 9$ and $f_i(x) = \mu_{i+1}$, $i = 1, 2, \ldots, 9$. See [3] for the details.

SIX-SPARSE STEINER TRIPLE SYSTEMS $v \equiv 9 \pmod{12}$ **[4]**

Construction

Let $v = 3p$, p prime, $p \equiv 3 \pmod 4$. Let ω be the square of a primitive root mod p such that $\omega \equiv 1 \pmod 3$. Let θ be the quadratic character of $\mathbb{F}_p$.

Choose α such that either (i) $\alpha \equiv 0 \pmod 3$ and $\theta(\alpha - 1) = 1$, or (ii) $\alpha \equiv 1 \pmod 3$ and $\theta(-\alpha) = 1$.

Then the set generated from $\{0, 1, \alpha\}$ and $\{0, p, 2p\}$ by the group of mappings $\langle x \mapsto \omega\, x,\ x \mapsto x + 1\rangle$ is the block set of an STS(v).

We call these *two-generator systems* because they are generated from two blocks. Alternatively, because for large p almost all the blocks of the system come from the orbit of $\{0, 1, \alpha\}$, we are tempted to call them *almost block transitive*.

Perfect system: Only one: $v = 33$, $\alpha = 7$, $\omega = 4$. **Big mystery: Why no more??**

6-sparse systems: Many!

v	α	v	α	v	α	v	α
489	135	501	160	1077	75	1101	379
1149	328	1329	309	1437	12	1461	13
1461	42	1509	490	1569	232	1641	223
1689	276	1857	141	1857	328	1929	502
1929	508	1941	3	1941	736	1977	519
2157	36	2157	186	2181	9	2217	193
2229	880	2361	979	2433	594	2589	684
2649	421	2649	609	2721	534	2733	24
2733	240	2733	585	2733	682	...	...

The special mitre configuration that we proved to be unavoidable in block transitive systems with $v \equiv 7 \pmod{12}$ does not form in the two-generator systems. Again using

Weil's theorem, we can prove that there is no such blocking mechanism to prevent the formation of 6-sparse two-generator systems of arbitrarily large orders.

Theorem 7 *For all sufficiently large v with $v = 3p$, p prime and $p \equiv 3 \pmod 4$, there exists α such that the system generated by $\{0, 1, \alpha\}$ and $\{0, p, 2p\}$ is 6-sparse.*

Theorem 8 *Let Λ be a finite set of polynomials such that no non-empty product of elements of Λ is a constant multiple of a square. Let $N > 0$.*
Then for all sufficiently large prime p, there exist N numbers α, distinct modulo p, such that $\theta(\lambda(\alpha)) = 1$ for all $\lambda(x) \in \Lambda$.

Proof. As before, with

$$\pi(x) = \prod_{\lambda(x)\in\Lambda} (1 + \theta(\lambda(x))) \quad \text{and} \quad \Delta = \sum_{x \bmod p} \pi(x). \qquad \square$$

Theorem 9 *Let $v = 3p$, p prime, $p \equiv 3 \pmod 4$. Then there exist a polynomial $Q(x)$ and a set Λ of polynomials such that no non-empty product of elements of Λ is a constant multiple of a square such that if α satisfies the following conditions:*

$\alpha \equiv 0 \pmod 3$,

$Q(\alpha) \not\equiv 0 \pmod p$ *and*

$\theta(\lambda(\alpha)) = 1$ *for all* $\lambda(x) \in \Lambda$,

then there exists a 6-sparse STS(v) generated by $\{0, 1, \alpha\}$ and $\{0, p, 2p\}$.

Proof. Hideous. Involves a massive amount of computation. We just give an example to illustrate the method. $\square$

The polynomial $Q(x)$ and the set of polynomials Λ play significant roles. In our lengthy analysis of the configurations relevant to 6-sparseness we encounter many polynomials $q(x)$ where it is a nuisance if $q(\alpha) = 0$. For example, these might occur as denominators, or as determinants of matrices. We bundle all these embarrassing polynomials $q(x)$ into the master polynomial, $Q(x)$, and by the choice of α we can assume that none of them has a zero at α, thus avoiding any trouble that such zeros might cause.

In fact the $Q(x)$ we constructed has degree four hundred and something, with coefficients often exceeding 100 digits. The first few factors are

$$Q(x) = x(x-3)(x-2)(x-1)(x+1)(x+2)(2x-3)(2x-1)(3x-2)(x^2+1)(x^2+2)\ldots.$$

Also we want to say something about the quadratic characters of certain rational functions of α that present themselves during the analysis. This is impossible without some predetermined assumptions. Suppose for some polynomial $\lambda(x)$ we desperately want to have $\theta(\lambda(\alpha)) = 1$ but we can't prove it. We avoid this difficulty by *assuming* that $\theta(\lambda(\alpha)) = 1$. We put all such polynomials $\lambda(x)$ into the set Λ. Then by our choice of α we can assume that $\theta(\lambda(\alpha)) = 1$ for all polynomials $\lambda(x) \in \Lambda$. However, we must be careful about putting things in Λ. To make Weil's theorem work, we must ensure that no non-empty product of polynomials in Λ is a constant multiple of a perfect square. For instance, putting both $f(x)$ and $-f(x)$ in Λ would be a very silly thing to do. Because of this constraint the construction of Λ is quite tricky.

The actual Λ used in [4] contains 28 polynomials, including x, $x-1$, $x+1$, $1-2x$, ...

Now for the example. Consider the 6-cycle (draw it!)

$$\{\{0,1,\alpha\},\{0,a,b\},\{e,\alpha,c\},\{e,b,d\},\{c,0,d\},\{a,e,1\}\}.$$

with the blocks ordered as written and assume all the blocks belong to the orbit of $\{0,1,\alpha\}$. We have the following set of equations.

$$\begin{aligned}
(0,a,b) &= (0,1,\alpha)\omega_1 + m_1,\\
(e,\alpha,c) &= (0,1,\alpha)\omega_2 + m_2,\\
(e,b,d) &= (0,1,\alpha)\omega_3 + m_3,\\
(c,0,d) &= (0,1,\alpha)\omega_4 + m_4,\\
(a,e,1) &= (0,1,\alpha)\omega_5 + m_5,
\end{aligned}$$

which on eliminating the m_i becomes

$$\begin{aligned}
-a+\omega_1 &= 0, & -b+\alpha\omega_1 &= 0,\\
e-\alpha+\omega_2 &= 0, & e-c+\alpha\omega_2 &= 0,\\
e-b+\omega_3 &= 0, & e-d+\alpha\omega_3 &= 0,\\
c+\omega_4 &= 0, & c-d+\alpha\omega_4 &= 0,\\
a-e+\omega_5 &= 0, & a-1+\alpha\omega_5 &= 0.
\end{aligned}$$

We want to show that these equations have no solution modulo $3p$ with $\omega_i \equiv 1 \pmod 3$ and $\theta(\omega_i) = 1$ for $i = 1,2,3,4,5$.

Mod 3. Working modulo 3, we can assume that $\alpha = 0$, $\omega_1 = \omega_2 = \cdots = \omega_5 = 1$. And indeed there is a unique solution: $a = 1,\ b = 0,\ c = 2,\ d = 2,\ e = 2$.

Mod p. So now we work modulo p. We put the equations into matrix form.

$$\begin{bmatrix}
-1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & -1 & 0 & 0 & 0 & \alpha & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & -1 & 0 & 1 & 0 & \alpha & 0 & 0 & 0\\
0 & -1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & -1 & 1 & 0 & 0 & \alpha & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\
0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & \alpha & 0\\
1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1\\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha
\end{bmatrix}
\begin{bmatrix} a\\ b\\ c\\ d\\ e\\ \omega_1\\ \omega_2\\ \omega_3\\ \omega_4\\ \omega_5 \end{bmatrix}
=
\begin{bmatrix} 0\\ 0\\ \alpha\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 1 \end{bmatrix}$$

The determinant is $\alpha(2\alpha-1)$. However, we had the foresight to include x and $2x-1$ in $Q(x)$. So we can assume that the determinant of the system of equations is non-zero modulo p. Hence there is a unique solution:

$$\omega_1 = \frac{-1+\alpha+\alpha^2-\alpha^3}{2\alpha-1}, \quad \omega_2 = \frac{\alpha^3-\alpha}{2\alpha-1}, \quad \omega_3 = \ldots.$$

But the solution must also satisfy

$$\theta(\omega_1) = \theta(\omega_2) = \theta(\omega_3) = \theta(\omega_4) = \theta(\omega_5) = 1.$$

Again with foresight we find that $x, x-1, x+1, 1-2x \in \Lambda$. So we can compute

$$\theta(\omega_2) = \theta(\alpha)\theta(\alpha-1)\theta(\alpha+1)\theta(2\alpha-1) = -1,$$

since $\theta(-1) = -1$. Hence for sufficiently large $p \equiv 3 \pmod 4$ there exists α such that the system generated by $\{0, 1, \alpha\}$ and $\{0, p, 2p\}$ does not contain the specific 6-cycle we have been considering.

To complete the proof of Theorem 9, all we need to do is examine a total of 2,303,423 further cases in a similar manner, adding polynomials to $Q(x)$ and Λ as explained above. Then by Theorem 8 we can choose α such that simultaneously $Q(\alpha) \neq 0$ and $\lambda(\alpha)$ is a square for all polynomials $\lambda(x) \in \Lambda$. The details are in [4].

CYCLIC ORDERED TRIPLEWHIST TOURNAMENTS

In an *ordered triplewhist tournament* of $4m + 1$ players, participants play a schedule of whist games. Each game (or table) involves four persons sitting in positions North, South, East and West. The players sitting North and South play as a partnership, opposing the players sitting East and West, who also play as a partnership. The schedule is arranged such that

1. there are $4m + 1$ rounds of m games each;
2. each player plays in exactly one game in all but one round;
3. each player partners every other player exactly once;
4. each player opposes every other player exactly once in a North-Westerly direction;
5. each player opposes every other player exactly once in a North-Easterly direction;
6. each player opposes every other player exactly once whilst sitting North or South;
7. each player opposes every other player exactly once whilst sitting East or West.

You can check that the numbers work.

In a *cyclic* ordered triplewhist tournament the players are numbers modulo $4m + 1$ and the schedule of the m games in round i, $i = 0, 1, \ldots, 4m$, is obtained by adding $i \pmod{4m + 1}$ to the elements of round 0.

Example [1]. A cyclic ordered triplewhist tournament with 29 players. We number the tables $0, 1, 2, 3, 4, 5, 6$. Then table i in the first round consists of players $(1, 3, 26, 13) = (3^{4i}, 3^{4i+1}, 3^{4i+15}, 3^{4i+26})$ sitting (North, West, South, East).

Yes, I had to expand the thing so that I could see the details of all 203 tables, and, yes, I did check that at least one of the players satisfies conditions 2–7. See page 13. Player i sits out during round i.

Exercise for reader: prove that this construction works either by checking every single entry on page 13 or by some other method.

A general construction [1]

Let $p = 8t + 5$ be prime and let ω be a primitive root modulo p. Then the first round defined by

$$\{(1, x, -1, x^3) \times \omega^i : i = 0, 4, 8, \ldots, 8t\},$$

where the ordering of the players is such that they sit (North, West, South, East), is the first round of an ordered triplewhist tournament provided x and $x^2 - 1$ are not squares modulo p and $x^2 \pm x + 1$ are squares but not fourth powers modulo p. (See [1] for explanation.)

So, again, we have a situation where we are looking for an x where simultaneously polynomial functions of x are various powers and non-powers in a finite field. And, as before, we can use Weil's theorem to prove that for all sufficiently large $p \equiv 5 \pmod 8$, there exists an x with the desired property and hence that the construction yields a cyclic ordered triplewhist tournament.

See the two papers by Ian Anderson and Leigh Ellison [1, 2] for details of this and other similar constructions.

References

[1] I. Anderson and L. Ellison, $\mathbb{Z}$-cyclic ordered triplewhist and directed triplewhist tournaments on p elements, where $p \equiv 5 \pmod 8$ is prime, *Discrete Math.* **293** (2005), 11–17.

[2] I. Anderson and L. Ellison, $\mathbb{Z}$-cyclic ordered triplewhist and directed triplewhist tournaments on p elements, where $p \equiv 9 \pmod{16}$ is prime, *J. Combin. Math. Combin. Comput.* **53** (2005), 39–48.

[3] A. D. Forbes, M. J. Grannell and T. S. Griggs, On 6-sparse Steiner triple systems, *J. Combin. Theory, Series A* **114** (2007), 235–252.

[4] A. D. Forbes, M. J. Grannell and T. S. Griggs, Further 6-sparse Steiner triple systems, submitted 2007.

[5] Wolfgang M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, *Lecture Notes in Mathematics* **536**, Springer–Verlag, 1976.

A cyclic ordered triplewhist tournament schedule for 29 players [1]

		01		23		07		16		20		25		24	
Round	0:	03	13	11	09	21	04	19	05	02	28	17	06	14	22
			26		18		08		10		27		12		15
		02		24		08		17		21		26		25	
Round	1:	04	14	12	10	22	05	20	06	03	00	18	07	15	23
			27		19		09		11		28		13		16
		03		25		09		18		22		27		26	
Round	2:	05	15	13	11	23	06	21	07	04	01	19	08	16	24
			28		20		10		12		00		14		17
		04		26		10		19		23		28		27	
Round	3:	06	16	14	12	24	07	22	08	05	02	20	09	17	25
			00		21		11		13		01		15		18
		05		27		11		20		24		00		28	
Round	4:	07	17	15	13	25	08	23	09	06	03	21	10	18	26
			01		22		12		14		02		16		19
		06		28		12		21		25		01		00	
Round	5:	08	18	16	14	26	09	24	10	07	04	22	11	19	27
			02		23		13		15		03		17		20
		07		00		13		22		26		02		01	
Round	6:	09	19	17	15	27	10	25	11	08	05	23	12	20	28
			03		24		14		16		04		18		21
		08		01		14		23		27		03		02	
Round	7:	10	20	18	16	28	11	26	12	09	06	24	13	21	00
			04		25		15		17		05		19		22
		09		02		15		24		28		04		03	
Round	8:	11	21	19	17	00	12	27	13	10	07	25	14	22	01
			05		26		16		18		06		20		23
		10		03		16		25		00		05		04	
Round	9:	12	22	20	18	01	13	28	14	11	08	26	15	23	02
			06		27		17		19		07		21		24
		11		04		17		26		01		06		05	
Round	10:	13	23	21	19	02	14	00	15	12	09	27	16	24	03
			07		28		18		20		08		22		25
		12		05		18		27		02		07		06	
Round	11:	14	24	22	20	03	15	01	16	13	10	28	17	25	04
			08		00		19		21		09		23		26

```
                13      06      19      28      03      08      07
Round 12:   15  25  23  21  04  16  02  17  14  11  00  18  26  05
                09      01      20      22      10      24      27

                14      07      20      00      04      09      08
Round 13:   16  26  24  22  05  17  03  18  15  12  01  19  27  06
                10      02      21      23      11      25      28

                15      08      21      01      05      10      09
Round 14:   17  27  25  23  06  18  04  19  16  13  02  20  28  07
                11      03      22      24      12      26      00

                16      09      22      02      06      11      10
Round 15:   18  28  26  24  07  19  05  20  17  14  03  21  00  08
                12      04      23      25      13      27      01

                17      10      23      03      07      12      11
Round 16:   19  00  27  25  08  20  06  21  18  15  04  22  01  09
                13      05      24      26      14      28      02

                18      11      24      04      08      13      12
Round 17:   20  01  28  26  09  21  07  22  19  16  05  23  02  10
                14      06      25      27      15      00      03

                19      12      25      05      09      14      13
Round 18:   21  02  00  27  10  22  08  23  20  17  06  24  03  11
                15      07      26      28      16      01      04

                20      13      26      06      10      15      14
Round 19:   22  03  01  28  11  23  09  24  21  18  07  25  04  12
                16      08      27      00      17      02      05

                21      14      27      07      11      16      15
Round 20:   23  04  02  00  12  24  10  25  22  19  08  26  05  13
                17      09      28      01      18      03      06

                22      15      28      08      12      17      16
Round 21:   24  05  03  01  13  25  11  26  23  20  09  27  06  14
                18      10      00      02      19      04      07

                23      16      00      09      13      18      17
Round 22:   25  06  04  02  14  26  12  27  24  21  10  28  07  15
                19      11      01      03      20      05      08

                24      17      01      10      14      19      18
Round 23:   26  07  05  03  15  27  13  28  25  22  11  00  08  16
                20      12      02      04      21      06      09

                25      18      02      11      15      20      19
Round 24:   27  08  06  04  16  28  14  00  26  23  12  01  09  17
                21      13      03      05      22      07      10
```

```
                26       19       03       12       16       21       20
Round 25:    28  09   07  05   17  00   15  01   27  24   13  02   10  18
                22       14       04       06       23       08       11

                27       20       04       13       17       22       21
Round 26:    00  10   08  06   18  01   16  02   28  25   14  03   11  19
                23       15       05       07       24       09       12

                28       21       05       14       18       23       22
Round 27:    01  11   09  07   19  02   17  03   00  26   15  04   12  20
                24       16       06       08       25       10       13

                00       22       06       15       19       24       23
Round 28:    02  12   10  08   20  03   18  04   01  27   16  05   13  21
                25       17       07       09       26       11       14
```