# DIFFERENCE SETS AND ALGEBRAIC NUMBER THEORY
## AN EXPOSITION OF SOME RESULTS OF SCHMIDT

GREGORY PRICE

Several combinatorical problems reduce to classifying certain families of *difference sets*. Schmidt, in [1], obtained strong new nonexistence results for this class of problem by applying algebraic number theory: a difference set can be related to a cyclotomic integer with bounded coefficients and a prescribed absolute value, and in many cases these integers can be number-theoretically proven not to exist. We lay out the core of Schmidt's results, simplifying what we can and omitting some of the less interesting details.

## 1. Difference Sets

A $(v, k, \lambda, n)$-difference set in a group $G$ of order $v$ is a $k$-subset $D \subset G$ such that each nonzero element of $G$ has exactly $\lambda$ representations as the difference of elements in $D$, with $n = k - \lambda$.

For instance, a *Hadamard matrix* is an $m \times m$ matrix $H$ with entries $\pm 1$ satisfying $H^T H = mI$. If we identify the row and column indices in the matrix with elements of an order-$m$ group $G$, then a *$G$-invariant Hadamard matrix* is a Hadamard matrix with $H_{g,h} = H_{fg,fh}$ for $f, g, h \in G$. Such a matrix is described by the entries $H_{1,g}$; if we let $D \subset G$ consist of the elements $g \in G$ with $H_{1,g} = 1$, then $D$ is a difference set with $v = m$; with some work it turns out that $n = m/4$ if $m > 2$.

In particular, we may consider *circulant Hadamard matrices*—Hadamard matrices invariant under cyclic groups $\mathbf{Z}/m\mathbf{Z}$. Such matrices are known only for $m = 1, 4$; it is known that any others must be of the form $4u^2$ for some $u$. A conjecture holds that there exist no circulant Hadamard matrices of order greater than 4. The results described herein will rule out almost all $u$ as candidates.

To study difference sets, we first describe a few preliminaries. We identify any set $S \subset G$ with the element $\sum_{g \in S} g$ of the integral group ring $\mathbf{Z}[G]$, and for any element $A = \sum_{g \in G} a_g g$ of the ring write $A^{(-1)}$ for $\sum_{g \in G} a_g g^{-1}$. A *character* of a finite abelian group $G$ is a homomorphism $\chi : G \to \mathbf{C}^*$ to the multiplicative group of nonzero complex numbers, hence to the group of $e$-th roots of unity for some $e$ called the *order* of $\chi$. We extend group homomorphisms $G \to H$ linearly to ring homomorphisms $\mathbf{Z}[G] \to \mathbf{Z}[H]$.

---

*Date*: 2004-05-24.

Now the condition that $D$ be a difference set becomes

$$DD^{(-1)} = n + \lambda G.$$

If we require $G$ to be abelian and apply any nontrivial character $\chi$ of $G$ to this equation we obtain

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

since $\chi(G) = 0$. A bit more generally, if we take a normal subgroup $U$ of $G$ with $G/U$ abelian and $\rho : G \to G/U$ the quotient map, then

$$\rho(D)\rho(D)^{(-1)} = n + \lambda|U|(G/U)$$

so for any nontrivial character $\chi$ of $G/U$

$$\chi(\rho(D))\overline{\chi(\rho(D))} = n.$$

So, writing $X$ for $\chi(\rho(D))$, $X\overline{X} = n$. But $X$ is a very particular sort of number; it's a cyclotomic integer, writable as $X = \sum_i a_i\zeta_m^i$ where $0 \leq a_i \leq |U|$ and $m$ is the order of $\chi$. For any particular $U$ and $m$, there are only finitely many of these, so the condition $X\overline{X} = n$ will turn out to be a restrictive one. We can use this to rule out classes of difference sets.

## 2. Bounding the Absolute Value of Cyclotomic Integers

We'll be concerned with the following version of the remaining problem: given a cyclotomic integer $X = \sum_i a_i\zeta_m^i \in \mathbf{Z}[\zeta_m]$ with $|a_i| < C$, for what $n \in \mathbf{Z}$ can $X\overline{X} = n$? For instance, by the triangle inequality, the complex absolute value of $X = \sum_i a_i\zeta_m^i$, $|a_i| \leq C$, is at most $mC$, so its square $X\overline{X}$ is at most $m^2C^2$. We thus have a bound on the possible values of $X\overline{X}$; we'll find others. For clarity we write the bounds we obtain as

$$X\overline{X} = n \leq M(m,n)C^2$$

(since they must scale quadratically with $C$); thus the bound we've already obtained is $M(m,n) = m^2$.

(Observe that we've given up the information that $a_i \geq 0$, which is true of all the cases arising from difference sets above. A careful analysis, keeping this information, gains about a factor of 2 in the bound $M$ obtained, but complicates the results that answer this question and the results that use the answer. For our purposes this isn't worth the loss in clarity.)

A sufficiently tight answer to this problem will allow us to rule out many possibilities for difference sets:

**Proposition 2.1.** *Let a group $G$ contain a $(v,k,\lambda,n)$-difference set $D$, and let $U$ be a normal subgroup of $G$ with $G/U$ cyclic of order $e$ and $\rho : G \to G/U$ be* *the quotient map. Then with $M(m,n)$ as above, we have*

$$e \leq \left(\frac{M(e,n)}{n}\right)^{1/2} v.$$

*Proof.* Let $\chi$ be a character of order $e$ on $G/U$. Since the homomorphism $\chi \circ \rho$ has kernel of order $v/e$, the image of $D$ can be written $\chi(\rho(D)) = \sum_{i=0}^{e-1} a_i \zeta_e^i$ with $0 \leq a_i \leq v/e$ and in particular $|a_i| \leq v/e$. Hence

$$n = \chi(\rho(D))\overline{\chi(\rho(D))} \leq M(e,n)\frac{v^2}{e^2}$$

which leads immediately to the result. □

We can be a bit more explicit in the abelian case, which follows immediately:

**Proposition 2.2.** *Let an abelian group $G$ contain a $(v,k,\lambda,n)$-difference set $D$. Then with $M(m,n)$ as above, we have*

$$\exp G \leq \left(\frac{M(v,n)}{n}\right)^{1/2} v$$

*where the* exponent $\exp G$ *of an abelian group $G$ is the order of its largest cyclic subgroup.*

In particular, if we have a circulant Hadamard matrix of order $m = 4u^2$, then $\exp G = v = 4u^2$ and $n = u^2$, so that

$$u \leq M(4u^2, u^2)^{1/2}.$$

Unfortunately, these results have little use for the trivial bound $M(m,n) = m^2$ found above; the resulting version of (2.1) is

$$n \leq v^2$$

which is uninteresting since in any case $n \leq k \leq v$. We'll need a better bound.

However, but for a constant factor, no better bound will come without using more specific information from the situation we're interested in. Indeed, taking $X = 1 + \zeta_m + \zeta_m^2 + \cdots + \zeta_m^{\lfloor m/2 \rfloor}$ gives for large $m$ a norm $|X| \simeq \frac{m}{\pi}$, so that $X\overline{X} \approx \pi^{-2}m^2$. What's going wrong in this case?

## 3. The Norm is Rational

The first refinement we can make is to observe that the absolute values $n$ we're interested in are rational integers. This means that once the absolute value is written in a basis (rather than the more-than-basis $\{\zeta_m^i\}_{i=0,\cdots,m-1}$), only the coefficient on 1 may be nonzero, and so the bound on each coefficient becomes a bound on the whole sum. It is straightforward to show that a bound $k$ on the coefficients in the more-than-basis implies a bound $2^{\delta(m)}k$ on the coefficients in the basis, where $\delta(m)$ is the number of distinct prime divisors of $m$. The bound on the more-than-basis coefficients in $X\overline{X}$ is $C^2m$, so

$$X\overline{X} \leq 2^{\delta(m)} m C^2,$$

and

$$M(m,n) = 2^{\delta(m)} m$$

works.

This, unfortunately, still gives us little in (2.1); the resulting inequality is

$$ne2^{-\delta(e)} \leq v^2$$

which is still uninteresting since in any case $ne2^{-\delta(e)} \leq v \cdot v \cdot 1 = v^2$.

This refinement, however, will help us after we make another one; and the fact that our $n$ of interest are rational will be essential in making the latter.

## 4. A Smaller Field

It turns out that for most $m$ and $n$, if $X\overline{X} = n$ lies in $\mathbf{Z}$ for some $X \in \mathbf{Z}[\zeta_m]$, then $X$ in fact lies, up to multiplication by a root of unity, in a much smaller cyclotomic field $\mathbf{Z}[\zeta_f]$. A bit more precisely,

**Theorem 4.1.** *If $X \in \mathbf{Z}[\zeta_m]$ satisfies $X\overline{X} = n \in \mathbf{Z}$, then in fact $X \in \zeta_m^j \mathbf{Z}[\zeta_{F(m,n)}]$ for some $j$, where $F$ is a function to be defined.*

It will turn out that $F$ is usually on the order of the squarefree part of $m$.

The proof of this depends on the following lemma, the most algebraic-number-theoretical of the results discussed in this paper. The *decomposition group* of a prime $P$ in a Galois extension $K/L$ is the subgroup of $\sigma$ in the Galois group with $P^\sigma = P$.

**Lemma 4.2.** *Let $P \mid p$ be prime ideals in $\mathbf{Z}[\zeta_m]$, $\mathbf{Z}$ respectively, and write $m = p^a m'$ with $p \nmid m'$. Then the decomposition group of $P$ over $\mathbf{Q}$ consists of exactly those $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$ that for some $j$ satisfy*

$$\sigma(\zeta_{m'}) = \zeta_{m'}^{p^j}.$$

Now write $m = \prod_i p_i^{c_i}$. We will define in terms of $m$ and $n$ a sequence of exponents $b_i \in \{1, \dots, c_i\}$ that are as small as we can make them while keeping the properties we need. We'll then outline a proof that for each $F_i = m/p^{c_i - b_i}$ we can write $X$ as a $p^{c_i}$-th root of unity $\xi_i$ (i.e. an element of the $F_j$, $j \neq i$) times an element of $\mathbf{Z}[\zeta_{F_i}]$. Writing $\xi = \prod_i \xi_i$ then gives $X\xi \in \mathbf{Z}[\zeta_{F_i}]$ for all $i$, so $X\xi \in \bigcap_i \mathbf{Z}[\zeta_{F_i}] = \mathbf{Z}[\zeta_F]$ where $F = \gcd_i F_i = \prod_i p_i^{b_i}$.

The property we need the $b_i$ to satisfy concerns automorphisms $\sigma_i : \zeta_m \mapsto \zeta_m^{1+F_i}$: each $\sigma_i$ must stabilize each prime ideal in $\mathbf{Z}[\zeta_m]$ lying over $n$. By the lemma on decomposition groups in cyclotomic fields, this is true if, for each prime $q \mid n$ and each $i$, $\zeta_{M_q}^{1+F_i} = \zeta_{M_q}^{q^l}$ for some power $l$, where $M_q = \prod_{p_j \neq q} p_j^{c_j}$. In other words, we need $1 + F_i \equiv q^l \pmod{M_q}$; if $p_i = q$ then $l = 0$ suffices, and otherwise we split this congruence into primes by the Chinese Remainder Theorem to obtain

$$\begin{aligned} 1 + p_i^{b_i} &\equiv q^l \pmod{p_i^{c_i}} \\ 1 &\equiv q^l \pmod{p_j^{c_j}} \qquad (p_j \neq p_i, q) \end{aligned}$$

For $p_i$ odd, we define $b_i$ to be the least integer such that these congruences are solvable. (We omit the case $p_i = 2$ for simplicity; it's a bit more complicated since the multiplicative groups modulo powers of 2 are in general not cyclic.) This is at most $c_i$, since $b_i = c_i$ makes $l = 0$ work. Otherwise, it's the exact power to which $p_i$ divides one less than the first power of $q$ satisfying $1 \equiv q^l \pmod{p_j^{c_j}}$ for all $j$ (which makes this power of $q$ generate the group of $1 + kp_i^{b_i}$ modulo $p_i^{c_i}$.)

Now, since the $\sigma_i$ stabilize each prime lying over $n$ and since $X\overline{X} = n$ so that each prime dividing $X$ divides also $n$, the $\sigma_i$ stabilize $X$. Hence each $X^{\sigma_i}$ is $X$ times a unit $\varepsilon_i$ of $\mathbf{Z}[\zeta_m]$. With some work it can be shown that this unit is in fact a root of unity; with some further work using only elementary modular arithmetic it can be shown that multiplying $X$ by a suitable $p_i^{c_i}$-th root of unity $\xi_i$ eliminates this unit factor and produces an $X\xi_i$ which is fixed by $\sigma_i$. So $X\xi_i$ lies in the fixed field of $\sigma_i$. This field certainly contains $\mathbf{Q}(\zeta_{F_i})$, since $\zeta_{F_i}^{\sigma_i} = \zeta_{F_i}^{1+F_i} = \zeta_{F_i}$; and by counting dimensions and applying the fundamental theorem of Galois theory, this is the entire fixed field. So $X\xi_i$ lies in $\mathbf{Q}(\zeta_{F_i})$ and hence, being an integer, in $\mathbf{Z}[\zeta_{F_i}]$.

We've now proven Theorem 4.1 modulo the lemma on decomposition groups, the case $p_i = 2$, and the details of showing that $X^{\sigma_i} = X\varepsilon_i$ implies the existence of $\xi_i$ with $(X\xi_i)^{\sigma_i} = X\xi_i$.

To apply this result to our main problem, it's some straightforward work to show that a bound $C$ on the coefficients of $X$ as a sum of powers of $\zeta_m$ implies the same bound $C$ on its coefficients as a sum of powers of $\zeta_{F(m,n)}$, using the fact that $F(m,n)$ contains all the same primes as $m$; then applying the result of Section 3 gives

$$X\overline{X} \leq 2^{\delta(F(m,n))} F(m,n) C^2 \leq 2^{\delta(m)} F(m,n) C^2,$$

so that

$$M(m,n) = 2^{\delta(m)} F(m,n)$$

works. The resulting version of (2.1) is

$$e \leq \left( \frac{2^{\delta(e)} F(e,n)}{n} \right)^{1/2} v$$

and in the circulant-Hadamard case

$$2u \leq 2^{\delta(2u)/2} F(4u^2, u^2)^{1/2}.$$

It remains to see just how much good this actually does us—nothing yet said has suggested that $F(m, n)$ is in general much smaller than $m$ itself, though by definition it can be no larger.

4.1. **How Much Smaller?** The first observation we can make about $F(m, n)$ is that it is independent of the powers to which primes occur in $n$ and nearly so in $m$; indeed, for any finite set of primes there is a finite bound on the value of $F(m, n)$ for $m, n$ products of powers of primes in the set. Hence for any choice of the primes making up $m$, $n$ we can make $F(m, n)$ much smaller than $m, n$ by taking these primes to large powers.

We can be a bit more specific by accepting some heuristicity, and by restricting to a common case. Write $m_0$ for the squarefree part of $m$, and let $n \leq m$, $m \approx m_0^2$, where '$\approx$' is used loosely. We'll show that for most such $m, n$, none of the large prime divisors of $m$ will occur more than once in $F(m, n)$. Schmidt claims in [1] that this makes $F(m, n)$ of the order of $m_0$ for such $m, n$. It's not obvious to me that it implies anything of the kind, especially since Schmidt defines the 'large' primes as those that are larger than the expected average of the prime powers in the factorization of $m$, and these primes are precisely the ones that usually occur only once in $m$ in the first place.

For a prime $q \mid n$, let $q^{o_{m_q}(q)}$ be the power of $q$ appearing in the definition of the $b_i$, where $m_q$ is the product of the $p_j$ distinct from $q$. Fix a prime $p_i \mid m$. Then $b_i > 1$ just if

$$p_i^2 \mid q^{o_{m_q}(q)} - 1$$

for some $q$. Now $o_{m_q}(q) \mid \phi(q)$, and most $p_i$ do not divide $\phi(q)$, so for any $n$ it is unlikely that any large $p_i$ divide $o_{m_q}(q)$. In the remaining cases, $Q \equiv 1 \pmod{p_i^2}$ only if $q$ lies in the subgroup of $(\mathbf{Z}/p^2\mathbf{Z})^*$ with order not divisible by $p$, which has $p - 1$ elements, a fraction $1/p$ of the total. Since large primes are nearly evenly distributed modulo each other, this happens a fraction $1/p$ of the time.

Now, excluding a set of density zero, any positive integer $x$ has approximately $\log \log x$ prime divisors. So outside of this set, we have no more than about $(\log \log m)(\log \log n) \approx (\log \log m_0)^2$ pairs $(p_i, q)$.

Now consider any 'large' $p_i$; Schmidt takes $p_i \geq m_0^{1/\log \log m_0} = \exp(\frac{\log m_0}{\log \log m_0})$, but we may take instead $p_i \geq \log m_0 = \exp(\log \log m_0)$, which is much smaller for large $m_0$. The probability that any of the divisions above for any of these primes holds is then at most $(\log \log m_0)^2/\log m_0$, which goes to zero for large $m_0$. For large $m_0$, then, we might hope that only a few small primes occur more than once in $F(m, n)$; i.e., that $F(m, n)$ is not much bigger than $m_0$.

What does this heuristic bound do for us in (2.1)? For $m \approx n \approx v$ and $m_0 \approx m^{1/2}$, we obtain

$$e \lessapprox \left( \frac{2^{\delta(e)} e^{1/2}}{n} \right)^{1/2} m$$

which in the abelian case becomes

$$e \lessapprox 2^{\delta(m)/2} m^{3/4} \approx m^{3/4}$$

since $\delta(m)$ grows very slowly with $m$.

In the case of circulant Hadamard matrices, this bound is quite powerful indeed. For when it applies, it requires

$$m \lessapprox m^{3/4}$$

which is false. Hence a circulant Hadamard matrix can only exist for $m$ on which this bound fails. Indeed, a circulant Hadamard matrix can only exist if $F(4u^2, u^2)$ is very nearly $4u^2$, and our heuristics suggest this should very rarely be the case. As expected, an explicit application of the bound, without heuristics, succeeds in ruling out nearly all $u$ for which it's been tried; for instance, only 26 values of $u$ less than 10000 are not ruled out, two between $10^5$ and $10^5 + 10^4$, and none at all between $10^8$ and $10^8 + 10^4$.

## References

[1] B. Schmidt: Cyclotomic integers and finite geometry. J. AMS 12 (1999), 929–952.