On Lander's Conjecture for Difference Sets whose Order is a Power of 2 or 3

Ka Hin Leung
Department of Mathematics
National University of Singapore
Kent Ridge, Singapore 119260
Republic of Singapore
matlkh@nus.edu.sg

Siu Lun Ma
Department of Mathematics
National University of Singapore
Kent Ridge, Singapore 119260
Republic of Singapore
matmasl@nus.edu.sg

Bernhard Schmidt
Division of Mathematical Sciences
School of Physical & Mathematical Sciences
Nanyang Technological University
Singapore 637371
bernhard@ntu.edu.sg

February 23, 2009

Abstract

Let p be a prime and let b be a positive integer. If a (v, k, λ, n) difference set D of order $n = p^b$ exists in an abelian group with cyclic Sylow p-subgroup S, then $p \in \{2, 3\}$ and $|S| = p$. Furthermore, either $p = 2$ and $v \equiv \lambda \equiv 2 \pmod 4$ or the parameters of D belong to one of four families explicitly determined in our main theorem.

1 Introduction

A $(\mathbf{v}, \mathbf{k}, \lambda, \mathbf{n})$ **difference set** in a finite group G of order v is a k-subset D of G such that every element $g \neq 1$ of G has exactly λ representations $g = d_1 d_2^{-1}$ with $d_1, d_2 \in D$. The positive integer $n = k - \lambda$ is called the **order** of the difference set. The existence of a (v, k, λ, n) difference set implies the existence of a symmetric (v, k, λ) design (see [2]). For detailed treatments of difference sets, see [1, 2, 3, 4, 5, 8].

Lander [5, p. 224] proposed the following conjecture.

Conjecture 1.1 (Lander 1983) *Let G be an abelian group of order v containing a difference set of order n. If p is a prime dividing v and n, then the Sylow p-subgroup of G cannot be cyclic.*

In [6, Thm. 1.3], the following was proved.

Result 1.2 *Lander's conjecture is correct in the case where n is a power of a prime $p > 3$.*

In the current paper, we obtain further progress towards Lander's conjecture in the case of difference sets of prime power order and prove the following result.

Theorem 1.3 *Let G be an abelian group of order v containing a (v, k, λ, n) difference set with $k < v/2$. Assume that n is a power of p where $p \in \{2, 3\}$, and that the Sylow p-subgroup S of G is cyclic. Then $n = p^{2t}$ for some positive integer t, and S has order p. Furthermore, one of the following holds.*

(*i*) $p = 2$ *and* $v \equiv \lambda \equiv 2 \pmod 4$.

(*ii*) $(v, k, \lambda, n) = (9 \cdot 2^{2t-1} - 2,\ 3 \cdot 2^{2t-1},\ 2^{2t-1},\ 2^{2t})$.

(*iii*) $(v, k, \lambda, n) = \left(\frac{25 \cdot 3^{2t-1} - 3}{2},\ 5 \cdot 3^{2t-1},\ 2 \cdot 3^{2t-1},\ 3^{2t}\right)$.

(*iv*) $(v, k, \lambda, n) = \left(\frac{49 \cdot 3^{2t-1} - 3}{4},\ \frac{7 \cdot 3^{2t} - 3}{4},\ \frac{3^{2t+1} - 3}{4},\ 3^{2t}\right)$.

(*v*) $(v, k, \lambda, n) = \left(\frac{64 \cdot 3^{2t-1} - 3}{5},\ \frac{8 \cdot 3^{2t} - 3}{5},\ \frac{3^{2t+1} - 3}{5},\ 3^{2t}\right)$.

2 Preliminaries

In this section, we list the definitions and basic facts we need in the rest of the paper. We first fix some notation. Let G be a finite group, and let R be a ring. We will always identify a subset A of G with the element $\sum_{g \in A} g$ of the group ring $R[G]$. For $B = \sum_{g \in G} b_g g \in R[G]$ we write $B^{(-1)} := \sum_{g \in G} b_g g^{-1}$ and $|B| := \sum_{g \in G} b_g$. We call $\{g \in G : b_g \neq 0\}$ the **support** of B. For $X, Y \in R[G]$, we write $X \subset Y$ if the support of X is contained in the support of Y. For $X \in R[G]$ and $g \in G$, the group ring element Xg is called a **translate** of X. A group homomorphism $G \to H$ is always assumed to be extended to a homomorphism $R[G] \to R[H]$ by linearity. For integers a, b, c, $b \geq 0$, we write $a^b || c$ if a^b, but not a^{b+1}, divides c.

Since D is a difference set in G if and only if $G \setminus D$ is a difference set in G, we can restrict our attention to (v, k, λ, n)-difference sets with $k \leq v/2$. Counting the number of quotients $d_1 d_2^{-1}$, $d_1, d_2 \in D$, $d_1 \neq d_2$, gives the trivial parameter condition $k(k-1) = \lambda(v-1)$. This implies that $k = v/2$ is impossible. Thus we can assume $k < v/2$. Note that in this case $\lambda < k/2$ and $n > k/2$ since $\lambda = k(k-1)/(v-1) < k^2/v < k/2$. Hence, throughout this paper, we will only consider difference sets with

$$k < \frac{v}{2} \text{ and } \lambda < \frac{k}{2} < n. \tag{1}$$

In the group ring language, difference sets can be characterized as follows [2, Lemma VI.3.2].

Result 2.1 *Let D be a k-subset of a group G of order v. Then D is a (v, k, λ, n) difference set in G if and only if in $\mathbb{Z}[G]$ the following holds.*

$$DD^{(-1)} = n + \lambda G \tag{2}$$

Notation 2.2 The following notation and assumptions will be used throughout the rest of the paper.

- $G = \langle \alpha \rangle \times H$ is an abelian group with cyclic Sylow p-subgroup $\langle \alpha \rangle$ where $p \in \{2, 3\}$.
- The order of α in G is p^s, $s \geq 1$.
- H is the complement of $\langle \alpha \rangle$ in G.
- $P = \langle \alpha^{p^{s-1}} \rangle$ is the unique subgroup of G of order p.
- D is a (v, k, λ, n) difference set in G where $n = p^r$ for some positive integer r, and (1) holds.
- If $p = 2$, then v is even and thus n is a square by Schützenberger's theorem [9]. So $r = 2t$ for some positive integer t. For $p = 2$ and $t \leq 2$, no difference set D as described above exists [2]. Thus we assume $r = 2t$ and $t \geq 3$ in the case $p = 2$.

3 Proof of Theorem 1.3

Let φ denote the Euler totient function. By [7, Theorem 4.3], we have

$$n \leq \begin{cases} \dfrac{4^2|H|}{4\varphi(4)} = 2|H| & \text{for } p = 2 \text{ and} \\ \dfrac{3^2|H|}{4\varphi(3)} = \dfrac{9|H|}{8} & \text{for } p = 3. \end{cases} \tag{3}$$

Lemma 3.1 *Let $p = 2$. Replacing D by a translate, if necessary, we have*

$$D = A + \alpha^{2^{s-1}} B + PC \tag{4}$$

with $A, B \subset H$ and $C \subset G$, such that A, B, and C are pairwise disjoint. Furthermore,

$$|A| = \frac{n+\sqrt{n}}{2}, \quad |B| = \frac{n-\sqrt{n}}{2} \quad \text{and} \quad |C| = \frac{\lambda}{2}. \tag{5}$$

Proof By [7, Thm. 4.1], we have $D = g(X - Y) + PZ$ with $X, Y \subset H$, $g \in G$, $Z \subset G$, and $X \cap Y = \emptyset$. Replacing D by Dg^{-1}, if necessary, we can assume $D = X - Y + PZ$. Since D has only non-negative coefficients, this implies $Y \subset PZ$. Hence, by replacing appropriate elements z of Z by $\alpha^{2^{s-1}} z$, if necessary, we can assume $Y \subset Z$. Hence we can write $Z = Y + T$ for some $T \subset G$. We have $D = X - Y + PZ = X - Y + P(Y + T) = X + \alpha^{2^{s-1}} Y + PT$. Taking $A = X$, $B = Y$, and $C = T$ shows that (4) holds. Note that A, B, and C are pairwise disjoint since D has coefficients 0 and 1 only.

Let $\rho : \mathbb{C}G \to \mathbb{C}H$ be the homomorphism defined by $\rho(\alpha) = e^{2\pi i/2^s}$ and $\rho(h) = h$ for $h \in H$. Then $\rho(D) = A - B$ by (4). Note that $\rho(G) = 0$. Using (2), we get

$$(A - B)(A - B)^{(-1)} = \rho(D)\rho(D)^{(-1)} = n. \tag{6}$$

This implies $|A| - |B| = \pm\sqrt{n}$. Comparing the coefficient of the identity element on both sides of (6) gives $|A| + |B| = n$. We conclude $\{|A|, |B|\} = \{(n - \sqrt{n})/2, (n + \sqrt{n})/2\}$. Replacing D by $\alpha^{2^{s-1}} D$, if necessary, we have $|A| = (n + \sqrt{n})/2$ and $|B| = (n - \sqrt{n})/2$. Since $k = |D| = |A| + |B| + 2|C| = n + 2|C| = k - \lambda + 2|C|$, we get $|C| = \lambda/2$ and thus (5) holds. **Q.E.D.**

We get a similar result in the case $p = 3$:

Lemma 3.2 *Let $p = 3$. Replacing D by a translate, if necessary, we have*

$$D = A + (P - 1)B + PC \tag{7}$$

with $A, B \subset H$, $C \subset G$, such that A, B, and C are pairwise disjoint. Furthermore, n is a square and

$$|A| = \frac{n+\delta}{2}, \quad |B| = \frac{n-\delta}{2} \quad \text{and} \quad |C| = \frac{1}{3}\left[\lambda - \left(\frac{n-\delta}{2}\right)\right] \tag{8}$$

where $\delta = \pm\sqrt{n}$.

Proof By Corollary 3.4, Lemma 3.6 and Theorem 4.2 of [6], we have

$$D = (X - Y)(P - 1) + PZ$$

for some $X, Y \subset H$ and $Z \subset G$ such that the supports of $X(P-1)$ and $Y(P-1)$ are disjoint. Since D has only nonnegative coefficients, this implies $Y(P-1) \subset PZ$. Recall $P = \langle \alpha^{3^{s-1}} \rangle$. Thus, by replacing suitable elements z of Z by $\alpha^{3^{s-1}}z$ or $\alpha^{2\cdot 3^{s-1}}z$, if necessary, we can assume $Y \subset Z$. Write $Z = Y + T$ with $T \subset G$. Then

$$D = (X - Y)(P - 1) + PZ = Y + X(P - 1) + PT.$$

Taking $A = Y$, $B = X$, and $C = T$ shows that (7) holds. Since D has coefficients 0 and 1 only, A, B, and C must be pairwise disjoint.

Let $\rho : \mathbb{C}G \to \mathbb{C}H$ be the homomorphism defined by $\rho(\alpha) = e^{2\pi i/3^s}$ and $\rho(h) = h$ for $h \in H$. Then $\rho(D) = A - B$ by (7). Note that $\rho(G) = 0$. Using (2), we get

$$(A - B)(A - B)^{(-1)} = \rho(D)\rho(D)^{(-1)} = n. \tag{9}$$

This implies that n is a square and $|A| - |B| = \pm\sqrt{n}$. Comparing the coefficient of the identity element on both sides of (9) gives $|A| + |B| = n$. We conclude $|A| = (n + \delta)/2$ and $|B| = (n - \delta)/2$ with $\delta = \pm\sqrt{n}$. Since $k = |D| = |A| + 2|B| + 3|C| = n + (n - \delta)/2 + 3|C| = k - \lambda + (n - \delta)/2 + 3|C|$, we get $|C| = (\lambda - (n - \delta)/2)/3$ and thus (8) holds. **Q.E.D.**

Lemma 3.3 *Let $p = 2$. We have $v \equiv 2 \pmod 4$, i.e., $s = 1$.*

Proof Recall that $n = 2^{2t}$ and $t \geq 3$. Assume $v \equiv 0 \pmod 4$, i.e., $s \geq 2$. Let $\mathbb{C}^*$ denote the multiplicative group of nonzero complex numbers, and let $\chi : \mathbb{Z}[G] \to \mathbb{C}^*$ be the homomorphism defined by $\chi(\alpha) = -1$ and $\chi(h) = 1$ for all $h \in H$. Note that $\chi(\alpha^{2^{s-1}}) = 1$ and thus $\chi(P) = 2$ since $s \geq 2$. Let U be the subgroup of G of index 2, and write $c_1 = |C \cap U|$, $c_2 = |C \cap U\alpha|$. Note that

$$c_1 + c_2 = |C| = \lambda/2 \tag{10}$$

by (5) and $\chi(C) = c_1 - c_2$. Furthermore, by (4) and (5), we have

$$\chi(D) = |A| + |B| + 2\chi(C) = n + 2\chi(C) = n + 2(c_1 - c_2). \tag{11}$$

From (10) and (11) we infer $4c_1 = \chi(D) - n + \lambda$ and $4c_2 = -\chi(D) + n + \lambda$. Since c_1 and c_2 are nonnegative, we conclude $\lambda \geq |n - \chi(D)|$. Since $\chi(D)$ is an integer, (2) implies $\chi(D) = \pm\sqrt{n}$, and thus we have

$$\lambda \geq n - \sqrt{n}. \tag{12}$$

Note that $v = (n^2 - n)/\lambda + 2n + \lambda$ since $(v-1)\lambda = k(k-1)$. Moreover, $n - \sqrt{n} \leq \lambda < n$ by (12). Since $f(\lambda) = (n^2 - n)/\lambda + 2n + \lambda$ is a convex function of λ, its maximum in the interval $[n - \sqrt{n}, n]$ is attained at one of the endpoints. This implies

$$2^s|H| = v \leq \max\{f(n - \sqrt{n}), f(n)\} = 4n. \tag{13}$$

On the other hand, for $n \geq 2$, we have $(n^2 - n)/x + 2n + x > 4n - 2$ for all $x \in \mathbb{R}^+$. Hence $v = (n^2 - n)/\lambda + 2n + \lambda > 4n - 2$. Together with (13), this implies $v \in \{4n - 1, 4n\}$. But $v = 4n - 1$ is impossible since v is even, and $v = 4n$ implies $|H| = 1$ and contradicts (3). **Q.E.D.**

Again, we will get a similar result for $p = 3$. We have seen before that n is a square in the case $p = 2$. By Lemma 3.2 this is also true for $p = 3$. Thus, from now on, we write $r = 2t$, i.e., $n = 3^{2t}$ if $p = 3$. Since $t = 1$ is impossible [2], we will assume $t \geq 2$ if $p = 3$.

Lemma 3.4 *Let $p = 3$. We have $v \equiv 3 \pmod 9$, i.e., $s = 1$. Furthermore,*

$$\lambda \geq \frac{n - \delta}{2} \quad \textit{and} \quad v \leq \frac{9n + 3\delta}{2}$$

where δ is defined in Lemma 3.2.

Proof Since $|C| \geq 0$, we have $\lambda \geq (n - \delta)/2$ by Lemma 3.2. Thus $(n-\delta)/2 \leq \lambda < n$. Note that $v = (n^2 - n)/\lambda + \lambda + 2n$ and that, as in the proof of Lemma 3.3, $f(\lambda)$ attains its maximum on the interval $[(n - \delta)/2, n]$ at one of the endpoints. Hence

$$3^s|H| = v \leq \max\{f((n - \delta)/2), f(n)\} = \frac{9n + 3\delta}{2}.$$

On the other hand, we have $n \leq 9|H|/8$ by (3) and thus $s = 1$. **Q.E.D.**

Lemma 3.5 *Either $p||\lambda$ or $p^{2t-1}||\lambda$.*

Proof Let $p=2$. Since $n=2^{2t}$ and $2|H|=v=(n^2-n)/\lambda+2n+\lambda$, we have $2^{4t}+2^{2t+1}\lambda+\lambda^2=2^{2t}+2\lambda|H|$. This implies the assertion since $t\geq 3$.

Now let $p=3$. The assertion follows from $\lambda<n$, $n=3^{2t}$, $\lambda^2+2\lambda n+n^2-n=\lambda v$, and $v\equiv 3 \pmod 9$. **Q.E.D.**

Lemma 3.6 *If $p=2$ and $2^{2t-1}||\lambda$, then*

$$(v,k,\lambda,n)=(9\cdot 2^{2t-1}-2,\ 3\cdot 2^{2t-1},\ 2^{2t-1},\ 2^{2t}).$$

If $p=3$ and $3^{2t-1}||\lambda$, then

$$(v,k,\lambda,n)=\left(\frac{25\cdot 3^{2t-1}-3}{2},\ 5\cdot 3^{2t-1},\ 2\cdot 3^{2t-1},\ 3^{2t}\right).$$

Proof Let $p=2$. Since $\lambda<n=2^{2t}$, we have $\lambda=2^{2t-1}$, $k=n+\lambda=3\cdot 2^{2t-1}$ and $v=(k^2-n)/\lambda=9\cdot 2^{2t-1}-2$.

Now let $p=3$. Since $\lambda<n$, we have $\lambda=3^{2t-1}$ or $2\cdot 3^{2t-1}$. If $\lambda=3^{2t-1}$, then $3^{2t-1}=\lambda\geq(n-\delta)/2=(3^{2t}\pm 3^t)/2$. But this implies $t=1$, contradicting our assumption $t\geq 2$. Thus we have $\lambda=2\cdot 3^{2t-1}$. Now the assertion follows from $k=n+\lambda$ and $\lambda(v-1)=k(k-1)$. **Q.E.D.**

Lemma 3.7 *If $p=3$ and $3||\lambda$, then either*

$$(v,k,\lambda,n)=\left(\frac{49\cdot 3^{2t-1}-3}{4},\ \frac{7\cdot 3^{2t}-3}{4},\ \frac{3^{2t+1}-3}{4},\ 3^{2t}\right)$$

or

$$(v,k,\lambda,n)=\left(\frac{64\cdot 3^{2t-1}-3}{5},\ \frac{8\cdot 3^{2t}-3}{5},\ \frac{3^{2t+1}-3}{5},\ 3^{2t}\right).$$

Proof As $v=(n^2-n)/\lambda+\lambda+2n$, we have $n-1\equiv 0 \pmod{\lambda/3}$. Write $y=3(n-1)/\lambda$. Since $\lambda<n$, we infer $y>3-3/n$. As y is not divisible by 3, we have $y\geq 4$.

On the other hand, $\lambda\geq(n-\delta)/2$ implies $y\leq 6(n-1)/(n-\delta)=6+6(\delta-1)/(n-\delta))=6+6/\delta$. Since we assume $t\geq 2$, we have $\delta\geq 9$, and thus we get $y<7$. Since $y\neq 6$, we conclude $y\leq 5$.

In summary, we have $y = \{4,5\}$ and hence $\lambda = (3^{2t+1} - 3)/4$ or $\lambda = (3^{2t+1} - 3)/5$. Now the assertion follows from $k = n + \lambda$ and $\lambda(v-1) = k(k-1)$. **Q.E.D.**

Proof of Theorem 1.3 This immediately follows from Lemmas 3.5, 3.6, and 3.7. **Q.E.D.**

Remark 3.8 For many values of t, standard results [2] can be used to show that difference sets with the parameters as stated in Theorem 1.3 cannot exist. However, it seems difficult to prove this for all t.

References

[1] L.D. Baumert: *Cyclic Difference Sets.* Springer Lecture Notes **182**, Springer 1971.

[2] T. Beth, D. Jungnickel, H. Lenz: *Design Theory* (2nd edition). Cambridge University Press 1999.

[3] D. Jungnickel: Difference Sets. *Contemporary Design Theory: A Collection of Surveys, eds. J.H. Dinitz, D.R. Stinson.* Wiley 1992, 241-324.

[4] D. Jungnickel, B. Schmidt: Difference Sets: An Update. *Geometry, Combinatorial Designs and Related Structures. Proc. First Pythagorean Conference, eds. J.W.P. Hirschfeld et al.* Cambridge University Press 1997, 89-112.

[5] E.S. Lander: *Symmetric Designs: An Algebraic Approach.* London Math. Soc. Lect. Notes **75**, Cambridge University Press 1983.

[6] K.H. Leung, S.L. Ma and B. Schmidt, Nonexistence of abelian difference sets: Lander's conjecture for prime power orders, *Trans. Amer. Math. Soc.*, 356 (2004), pp. 4343-4358.

[7] K.H. Leung and B. Schmidt, The Field Descent Method, *Des. Codes Cryptogr.*, 36 (2005), pp. 171-188.

[8] A. Pott: *Finite geometry and character theory.* Springer Lecture Notes **1601**, Springer 1995.

[9] M.P. Schützenberger: A nonexistence theorem for an infinite family of symmetrical block designs. *Ann. Eugen.* **14** (1949) 286-287.