A Note on BIB Designs with Nested Rows and Columns

James A. MacDougall

Department of Mathematics
University of Newcastle, NSW 2308, Australia

Gary L. Mullen

Department of Mathematics
Pennsylvania State University, University Park, PA 16802-6401, USA

Abstract

In [1] Aggarwal & Arasu devised a construction for balanced incomplete block designs having nested rows and columns. Their construction uses finite fields and depends on the existence of primitive elements having certain properties. They conjectured that such primitive elements always exist. The purpose of this short note is to point out that their conjecture is true.

The purpose of this note is to confirm a conjecture raised by Aggarwal & Arasu concerning the existence of certain block designs. In their paper [1] they provide a construction for a family of balanced incomplete block designs having nested rows and columns (BIBRC). A BIBRC is an arrangement of v treatments into b blocks satisfying the conditions:
(i) each block is a $s \times t$ array of st plots,
(ii) every treatment occurs at most once in each block,
(iii) every treatment occurs in exactly r blocks,
(iv) for every pair of treatments $i \neq j$,

$$s\lambda_{i,j}^R + t\lambda_{i,j}^C - \lambda_{i,j} = \lambda = \frac{r(s-1)(t-1)}{v-1}$$

where $\lambda_{i,j}^R$ and $\lambda_{i,j}^C$ denote, respectively, the number of rows and columns of the blocks in which the treatment pair (i,j) occurs, and $\lambda_{i,j}$ denotes the number of blocks in which the ordered pair (i,j) occurs. Such a design will be denoted $BIBRC(v,b,r,s,t,\lambda)$.

The construction explained in [1] builds a design of 2-row ($s = 2$) blocks from a single starter block. The resulting design has parameters $b = v$, $r = v - 1$, $s = 2$,

$t = \frac{v-1}{2}$ and $\lambda = \frac{v-3}{2}$. For the starter block to generate the design, there must be an element x in the finite field F_q, $q \equiv 5 \pmod 8$, with the properties:

(i) x is a primitive element,

(ii) $x^2 - 1$ is a square.

They conjecture (*Remark 1* of [1]) that such an element always exists. This conjecture is interesting in its own right apart from its application. Properties of this kind have been studied for some time by a number of authors and readers are referred to [3] for a survey. We point out that this particular conjecture follows from a theorem of S. D. Cohen on values of polynomials over finite fields. The following result appears as Theorem 1.3 of [2]:

Theorem 1 *If $g(x)$ is a quadratic polynomial over F_q not of the form $a(x+b)^2$ where a is a non-square in F_q and $q \notin A$, then $g(\omega)$ is a non-zero square in F_q for some primitive root ω of F_q.*

The set of exceptions to Theorem 1 is $A = \{2, 3, 4, 5, 7, 9, 11, 13, 19, 25, 31, 37, 43, 49, 61, 67, 121, 211\}$. A proof of the conjecture follows by applying Theorem 1 with $g(x) = x^2 - 1$ and checking that, for this particular polynomial, there are no small exceptions. This now enables us to strengthen Theorem 1 of [1] to:

Theorem 2 *Let $v \equiv 5 (\mathrm{mod}\, 8)$ be a prime or prime power. Then there exists a BIBRC with parameters $(v, v, v-1, 2, \frac{v-1}{2}, \frac{v-3}{2})$.*

In support of their conjecture in [1], the authors gave an example of a primitive element in F_p having the required propery, for each prime p less than 1000. In fact, such elements are plentiful. In the following table, we tabulate the total number, N(p), of such elements along with the smallest one, g, for each prime $p \equiv 5 \pmod 8$ with $p < 1000$. Asymptotically the number of such primitive elements in the finite field F_q should be $\phi(q-1)/2$. In fact methods from [2] could be used to obtain results along these lines for large q.

p	g	N(p)	p	g	N(p)	p	g	N(p)
13	2	4	277	11	40	661	2	88
29	8	4	293	5	64	677	5	160
37	2	4	317	5	84	701	8	112
53	5	16	349	2	56	709	2	120
61	2	8	373	2	64	733	6	144
101	11	16	389	8	88	757	2	104
109	6	20	397	6	56	773	2	184
149	8	40	421	2	56	797	5	204
157	6	24	461	11	104	821	8	152
173	5	36	509	10	124	829	2	144
181	2	24	541	2	56	853	2	128
197	5	44	557	5	148	877	2	136
229	7	40	613	2	96	941	11	152
169	10	60	563	5	156	997	3	160

References

[1] Aggarwal, M. L. & Arasu, K. T., *A New Family of Balanced Incomplete Block Designs With Nested Rows and Columns*, Australas.J.Combin., **12** (1995), 295-299

[2] Cohen, Stephen D., *Primitive roots and powers among values of polynomials over finite fields*, J. Reine Angew. Math. **350** (1984), 137–151.

[3] Cohen, Stephen D., *Primitive elements and polynomials: existence results.* Finite fields, coding theory, and advances in communications and computing (Las Vegas, NV, 1991), 43–55, Lecture Notes in Pure and Appl. Math., 141, Dekker, New York, 1993

(Received 18/2/99)