A few more small defining sets for SBIBD$(4t-1, 2t-1, t-1)$

Thomas Kunkle
Department of Mathematics
College of Charleston
Charleson, SC
USA 29424
email: kunkle@math.cofc.edu

Jennifer Seberry*
Department of Computer Science
The University of Wollongong
Wollongong, NSW, 2500
Australia
email: j.seberry@uow.edu.au

ABSTRACT. It has been conjectured by Dinesh Sarvate and Jennifer Seberry, that, when p is an odd prime or prime power congruent to 1 mod 4, a certain collection of p sets of p elements can be used to define uniquely an SBIBD$(2p+1, p, \frac{1}{2}(p-1))$, and that, when p is a prime power congruent to 3 mod 4, then a certain collection of $\frac{1}{2}(p-1)$ sets can be used to define uniquely an SBIBD$(p, \frac{1}{2}(p-1), \frac{1}{4}(p-3))$. This would mean that, in certain cases, $2t-1$ rows are enough to complete uniquely the Hadamard matrix of order $4t$. Examples suggest that the defining sets can be used first to find the corresponding residual BIBD, which can then be extended uniquely to the SBIBD.

These conjectures have now been verified for p =5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, 43, 47, 59 and 67, providing further examples in which a residual design with $\lambda > 2$ is completable to an SBIBD, the first such case having been given in Seberry in 1992.

*Research funded by ARC grant A48830241 and an ATERB grant.

We will refer to a design and its incidence matrix, with treatments as rows and blocks as columns, interchangeably.

Smallest defining sets have been studied by Gray [1, 2, 3] and Gray and Street [4]. Other minimal defining sets in Hadamard matrices and their residuals by Sarvate and Seberry [?, ?]. Definitions are used from [?, ?, ?].

1. The case $p \equiv 1 \pmod 4$

Suppose that $p = 4t + 1 = q^r$ is a prime power congruent to 1 modulo 4; we recall that a Galois field $GF(q^r)$ generated by the minimal polynomial g and irreducible element x, is a field consisting of the polynomials in x modulo g with integer coefficients modulo q.

Let $D = \{x^2, x^4, \ldots, x^{2t}\}$, the quadratic residues of $GF(q^r)$. Define E to be the ordered set $\{D, p + D\}$, i.e.,

$$E = \{x^2, x^4, \ldots, x^{2t}, p, p + x^2, p + x^4, \ldots, p + x^{2t}\}.$$

We adopt the following convention. Among the first $2t$ elements of E, all coefficients are reduced modulo q to lie in between 0 and $q - 1$. However, among the last $2t + 1$ elements, the coefficients of the polynomial elements are reduced modulo q to lie between 0 and $q - 1$ while the constant term is reduced to lie between p and $p + q - 1$.

We next construct a $p \times 2p$ partial incidence matrix by first labeling its rows by the elements of $GF(q^r)$ and its columns by the elements of $\{GF(q^r), p + GF(q^r)\}$ and then specifying, for each row index, a particular collection of the column indices.

For each $i \in GF(q^r)$, define

$$E_i = i + E,$$

a subset of $\{GF(q^r), p + GF(q^r)\}$, where the addition of i to each element of E is taken mod $(g(x), q)$ as described earlier.

Conjecture 1 *If $p = q^r \equiv 1 \pmod 4$ is a prime power, then the collection $\{E_i : i \in GF(q^r)\}$ is a minimal defining set for an SBIBD$(2p + 1, p, \frac{1}{2}(p - 1))$.*

This note is to record the fact that this conjecture is true for for $p = 25$ and 29 as well as the previously known $p = 5$, 9, 13, and 17. The result was obtained by generating the initial sets $\{E_i\}$, using them to construct the associated rows of zeros and ones, and then finding all vectors of p ones and $p + 1$ zeros which have $\frac{1}{2}(p - 1)$ columns where both the new row and a row constructed from E_i contain a one. This must be true for each i. There were exactly $\frac{1}{2}(p + 1)$ such rows and, when combined with $\{E_i\}$, they formed the desired SBIBD.

This is further evidence for the conjecture:

Conjecture 2 *The collection in Conjecture 1 forms the residual design of an* $SBIBD(2p+1, p, \frac{1}{2}(p-1))$.

2. The case $p \equiv 3 \pmod 4$

Seberry [?] gave a conjecture for primes p equivalent to 3 modulo 4 and showed the conjecture is true for $p = 7$, 11, and 19. Subsequently Gower [?] showed the conjecture is true for $p = 23$. The conjecture was extended in [?] to the case of prime powers.

Conjecture 3 *Let* $p = 4t-1$, *a prime power, let* x *be an irreducible element in* $GF(p)$, *and let* $E_0 = \{x^2, x^4, \ldots, x^{4t-2}\}$, *the set of quadratic residues in this field. For* $0 < i < 2t$, *define* $E_i = x^{2i} + E_0$.

Then $\{E_0, \ldots, E_{2t-1}\}$ *is the residual design of an* $SBIBD(4t-1, 2t-1, t-1)$.

Conjecture 4 *Suppose* $4t-1$ *is a prime power. Then the sets* $E_1, \ldots, E_{2t-1}$ *can be extended using the link property of blocks of an SBIBD to form an* $SBIBD(4t-1, 2t-1, t-1)$. *This extension is unique up to permutation of treatments.*

This note is to record the fact that this conjecture is true for for $p =$ 27, 43, 47, 59, 67 as well as the previously known $p = 7$, 11, 19, and 23. This was verified by generating the sets E_i, using them to construct the associated rows of zeros and ones, and then finding all vectors of $\frac{1}{2}(p-1)$ ones and $\frac{1}{2}(p+1)$ zeros which have $\frac{1}{2}(p-3)$ columns where both the new row and a row constructed from E_i contain a one. This must be true for each i. There were exactly $\frac{1}{2}(p+1)$ such rows and, when combined with $\{E_i\}$, they formed the desired SBIBD.

References

[1] Ken Gray, Further results on smallest defining sets of well known designs, *Australas. J. Combinatorics* 1:91–100, 1990.

[2] Ken Gray, On the minimum number of blocks defining a design, *Bull. Austral. Math. Soc.* 41:97–112, 1990.

[3] Ken Gray, Defining sets of single-transposition-free designs, *Utilitas Math.* 38:97–103, 1990.

[4] Ken Gray and Anne Penfold Street, Smallest defining sets of the five non- isomorphic $2-(15,7,3)$ designs, *Bull. ICA*, 9:96–102, 1993.

[5] Rebecca Gower, e-mail communication to Jennifer Seberry, Nov 1991.

[6] Dinesh Sarvate and Jennifer Seberry, A note on small defining sets for some SBIBD($4t-1,\ 2t-1,\ t-1$), *Bull. ICA*, 10:26–32, 1994.

[7] Jennifer Seberry, On small defining sets for some SBIBD($4t-1,\ 2t-1,\ t-1$), *Bull. ICA*, 4:58–62, 1992; corrigendum, *Bull. ICA*, 6:62, 1992.

[8] Jennifer Seberry Wallis, Hadamard matrices, Part IV, *Combinatorics: Room Squares, Sum free sets and Hadamard Matrices*, Lecture Notes in Mathematics, Vol 292, eds. W. D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, Springer-Verlag, Berlin-Heidelberg-New York, 1972.

[9] Thomas Storer, *Cyclotomy and Difference Sets*, Lectures in Advanced Mathematics, Markham, Chicago, 1967.

[10] T. Tsuzuku, *Finite Groups and Finite Geometries*, Cambridge University Press, Cambridge, 1982.