J Comb Optim (2008) 15: 1–6
DOI 10.1007/s10878-007-9079-z

Steiner systems for two-stage disjunctive testing

Vladimir D. Tonchev

Published online: 6 July 2007

Abstract The subject of this paper are some constructions of Steiner designs with blocks of two sizes that differ by one. The study of such designs is motivated by a combinatorial lower bound on the minimum number of individual tests at the second stage of a 2-stage disjunctive testing algorithm.

Keywords Group testing · Two-stage testing algorithm · Steiner design

1 A two-stage disjunctive testing algorithm

The fundamental group testing problem (Du and Hwang 1993) can be described in a simplified form as follows: Given a set S of n objects and unknown subset P of S whose elements are considered as *defective*, or *positive*, the task is to determine P by its intersections with a given collection of known subsets of S.

Disjunctive testing is a technique for implementing group testing that employs Boolean operations. The purpose is to find the unknown subset P by reconstructing its binary $(0, 1)$-incidence vector $x = (x_1, \ldots, x_n)$, where $x_i = 1$ if the ith object belongs to P and $x_i = 0$ otherwise. The reconstruction of x can be achieved by applying a two-stage disjunctive testing process (Levenshtein 2003) that works as follows. At the first stage, disjunctive tests are performed that are determined by the rows of an $m \times n$ binary matrix $H = (h_{i,j})$. The matrix H plays a role similar to that of a parity-check matrix of a binary linear code: one attempts to recover x from the syndrome

$$s = xH^T,$$

V.D. Tonchev (✉)
Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931, USA
e-mail: tonchev@mtu.edu

where the matrix product is computed by using the logical operations disjunction $\vee$ and conjunction &, and $s = (s_1, \ldots, s_m)$, where

$$s_i = \bigvee_{j=1}^{n} x_j \,\&\, h_{i,j}, \quad i = 1, \ldots, m.$$

Let $I_n = \{1, 2, \ldots, n\}$, $F = \{0, 1\}$, and let X be the support of $x = (x_1, \ldots, x_n)$:

$$X = \{i \in I_n : \ x_i = 1\}.$$

The elements of X are the active items of x. Thus, $s_i = 0$ if X and the set H_i of active items of the ith row $h_i = (h_{i,1}, \ldots, h_{i,n})$ of H are disjoint, and $s_i = 1$ otherwise.

Given a syndrome $s = (s_1, \ldots, s_m)$, let $Q(H, s)$ be the set of all vectors x having syndrome equal to s, i.e.

$$Q(H, s) = \{x \in F^n \mid s = xH^T\}.$$

If it happens that the syndromes of all $x \in F^n$ of Hamming weight t or less are distinct, one can reconstruct $x \in F^n$ provided that its weight is at most t. In this case, the columns of H are said to form a *t-disjunctive code*. An item $i \in I_n$ is positive if $y_i = 1$ for all $y \in Q(H, s)$, and an item $i \in I_n$ is negative if $y_i = 0$ for all $y \in Q(H, s)$. All remaining $u(H, x)$ items $i \in I_n$ are unresolved.

A two-stage disjunctive testing algorithm for reconstructing x computes $Q(H, s)$ and determines the positive, negative and unresolved items at Stage 1, and conducts individual tests at Stage 2 to determine which of the remaining $u(H, x)$ unresolved items from Stage 1 are positive or negative.

2 A lower bound on the number of tests

We assume that the choice of $x \in F^n$ is governed by a Bernoulli probability distribution P with parameter p, $0 < p < 1$. The efficiency of the two-stage testing algorithm is characterized by the average number

$$E(H, p) = m + \tilde{u}(H, p)$$

of tests used to determine an unknown $x \in F^n$, where

$$\tilde{u}(H, p) = \sum_{x \in F^n} u(H, x) P(x).$$

The optimization problem that arises is to find

$$E(n, p) = \min E(H, p) = \min(m + \tilde{u}(H, p)),$$

where the minimum is taken over all matrices H with n columns and any number $m \geq 1$ of rows.

The problem of optimal selection of matrices H for two-stage disjunctive testing was studied by Levenshtein (2003), who proved the following lower bound on $\tilde{u}(H, p)$:

$$\tilde{u}(H, p) \geq n \sum_{i=1}^{n} \binom{n}{i} p^i (1-p)^{n-i} 2^{-\frac{m}{i}} - np. \tag{1}$$

Let X be the set of active items of $x \in F^n$, let $\bar{x}$ be a vector in F^n of maximum Hamming weight that has the same syndrome as x, that is, $s = xH^T = \bar{x}H^T$, and let $\bar{X}$ be the set of active items of $\bar{x}$. Then $X \subseteq \bar{X}$ and $\bar{X} \setminus X$ consists of unresolved items. It follows that

$$\tilde{u}(H, p) \geq \sum_{x \in F^n} |\bar{X} \setminus X| P(x).$$

The proof of this bound is based on a combinatorial problem described below.

A combinatorial t-design $\mathcal{D} = (S, \mathcal{B})$ of index λ is a finite set S of *points* together with a collection of subsets $\mathcal{B} = \{B \mid B \subseteq S\}$ called *blocks* such that every t-subset of S is contained in exactly λ blocks from $\mathcal{B}$. A t-(n, K, λ) is a t-design with n points and block sizes $K = \{|B| : B \in \mathcal{B}\}$. A t-(n, k, λ) design is a design with $K = \{k\}$. A Steiner design (or Steiner *system*) is a t-design with $\lambda = 1$. A t-(n, k, λ) design is *trivial* (or *complete*) if the collection of blocks consists of all k-subsets.

Let $V(n)$ be the collection of all 2^n subsets of I_n, and let $V_i(n) = \{X \in V(n) : |X| = i\}$ be the collection of all i-subsets of I_n. For a fixed i $(1 \leq i \leq n)$, consider a covering operator $F : V_i(n) \to V(n)$ such that $X \subseteq F(X)$ for any $X \in V_i(n)$.

Let

$$C = \{F(X) : X \in V_i(n)\}.$$

For any T, $1 \leq T \leq \binom{n}{i}$, consider the decreasing continuous function $g_i(T) = k + (k+1)(1-\alpha)/i$, where k and α are uniquely determined by the equations $T\binom{k}{i} = \alpha\binom{n}{i}$, where $k \in \{i, \ldots, n\}$, and $1 - i/(k+1) < \alpha \leq 1$. The inequality (1) is a corollary of the following combinatorial bound.

Theorem 2.1 (Levenshtein 2003)

$$\frac{1}{\binom{n}{i}} \sum_{x \in V_i(n)} |F(x)| \geq g_i(|C|), \tag{2}$$

with equality if and only if C is a Steiner system i-$(n, \{k, k+1\}, 1)$.

3 Steiner designs with two block sizes

Theorem 2.1 motivates the interest in Steiner systems with blocks of two different sizes. A trivial way to obtain a t-$(n, \{k, k+1\}, 1)$ design is by deleting a point from a given t-$(n+1, k+1, 1)$ design. Currently, only finitely many nontrivial Steiner 4- or 5-designs with constant block size are known, and no Steiner t-$(n, k, 1)$ design is known if $t > 5$ and $k > t$. The following are two infinite classes of nontrivial Steiner designs with $t = 5$ and $t = 4$ having blocks of two different sizes:

- 5-$(2^n, \{6, 8\}, 1)$, $n \geq 4$ (Wilson 1972a, 1972b, 1975).
- 4-$(4^n + 1, \{5, 6\}, 1)$, $n \geq 2$ (Tonchev 1996).

In the rest of this paper, we consider some combinatorial constructions of Steiner designs with two block sizes that differ by one obtained from Steined designs that contain substructures of certain type.

A design $\mathcal{D}' = (S', \mathcal{B}')$ is a *subdesign* of $\mathcal{D} = (S, \mathcal{B})$ if $S' \subseteq S$ and $\mathcal{B}' \subseteq \mathcal{B}$.

Theorem 3.1 *Suppose that $\mathcal{D} = (S, \mathcal{B})$ is a Steiner t-$(n, k, 1)$ design that contains a Steiner $(t-1)$-$(n, k, 1)$ subdesign $\mathcal{D}' = (S, \mathcal{B}')$. Then the blocks of $\mathcal{D}'$, each extended with one new point s^*, $s^* \notin S$, together with the blocks of $\mathcal{D}$ that do not belong to $\mathcal{D}'$, form a Steiner t-$(n+1, \{k+1, k\}, 1)$ design.*

The proof is straightforward and therefore omitted.

A *parallel class* in a t-(kt, k, λ) design D is a set of t pairwise disjoint blocks that partition the point set of D. A design is *resolvable* if its collection of blocks can be partitioned into disjoint parallel classes.

Since the blocks of a parallel class form a Steiner 1-design, we have the following.

Corollary 3.2 *If a Steiner 2-$(kt, k, 1)$ design with a parallel class exists then there exists a Steiner 2-$(kt+1, \{k+1, k\}, 1)$ design.*

For every prime power q and every integer $n \geq 2$, there exists a resolvable 2-$(q^n, q, 1)$ design having as blocks the lines in a finite affine geometry $AG(n, q)$. Thus, Corollary 3.2 implies the following result.

Corollary 3.3 *A Steiner 2-$(q^n+1, \{q, q+1\}, 1)$ design exists for every prime power q and every integer $n \geq 2$.*

It is known that a resolvable 2-$(6m+3, 3, 1)$ design (or a Steiner Kirkman system) exists for every integer $m \geq 1$. Thus, using Corollary 3.2, we have the following.

Corollary 3.4 *A Steiner 2-$(6m+4, \{3, 4\}, 1)$ design exists for every integer $m \geq 1$.*

4 Some Steiner 3-designs with two block sizes

The largest value of t for which infinitely many nontrivial Steiner t-designs with a constant block size are known to exist is $t = 3$.

It is known that a Steiner 3-$(n, 4, 1)$ design or a Steiner Quadruple System $SQS(n)$ exists if and only if $n \equiv 2, 4 \pmod 6$.

An $SQS(n)$ is *2-resolvable* if its blocks can be partitioned into disjoint Steiner 2-$(n, 4, 1)$ designs.

The classical $SQS(2^{2m})$ having as blocks the planes in $AG(2m, 2)$, $m \geq 2$, is 2-resolvable (Baker 1976; Semakov et al. 1973). Applying Theorem 3.1 to the classical 2-resolvable $SQS(2^{2m})$, we have the following.

Corollary 4.1 *For every $m \geq 2$ there exists a Steiner 3-$(2^{2m}+1, \{4, 5\}, 1)$ design.*

Table 1 $SQS(16)$ of 2-rank 11 and 12

# SQS	2-rank	# 2-(16,4,1) subdesigns	2-resolvable	# 2-resolutions
1, $AG(4,2)$	11	56	Yes	240
1	12	56	Yes	64
4	12	24	No	0
5	12	8	No	0
5	12	0	No	0

Some recursive constructions of other 2-resolvable $SQS(n)$ were given by Teirlinck (1994).

Theorem 4.2 (Teirlinck 1994) *A 2-resolvable* $SQS(2\cdot 7^n+2)$ *exists for every* $n \geq 1$.

Theorem 3.1 and Teirlinck's result imply the following.

Corollary 4.3 *A Steiner* 3-$(2\cdot 7^n+3, \{4,5\}, 1)$ *design exists for every* $n \geq 1$.

We note that the requirement for an $SQS(n)$ to have a Steiner 2-subdesign is weaker than to be 2-resolvable. Table 1 provides information about 2-subdesigns and 2-resolvability of Steiner quadruple systems on 16 points having incidence matrices of 2-rank 11 or 12. As shown in Tonchev (2003), there are sixteen non-isomorphic such designs.

Another known infinite family of Steiner 3-designs consists of 3-$(q^n+1, q+1, 1)$ designs, where q is an arbitrary prime power and $n \geq 2$, obtained from spherical geometries (cf. Beth et al. 1999; Colbourn and Dinitz 1996). Applying Theorem 3.1 to these designs, we have the following.

Proposition 4.4 *The existence of a spherical* 3-$(q^n+1, q+1, 1)$ *design having a* 2-$(q^n+1, q+1, 1)$ *subdesign implies the existence of a Steiner* 3-$(q^n+2, \{q+1, q+2\}, 1)$ *design*.

A necessary condition for a 3-$(q^n+1, q+1, 1)$ design to contain a 2-$(q^n+1, q+1, 1)$ subdesign is that n is odd. Thus, $n = 2t+1,\ n \geq 3$.

A 2-$(q^3+1, q+1, 1)$ is called a *unital*. Unitals are known to exist for every prime power q, as well as for $q = 6$.

In view of the above construction, it is an interesting open question when a spherical 3-$(q^3+1, q+1, 1)$ design contains a unital 2-$(q^3+1, q+1, 1)$. The answer is known to be in the affirmative for the smallest case $q = 3$.

Theorem 4.5 (Mathon, private communication) *There exists a* 3-$(28, 4, 1)$ *design with a* 2-$(28, 4, 1)$ *subdesign*.

5 Conclusion

The optimization problem of minimizing the number of unresolved items in a 2-stage disjunctive testing algorithm motivates the study of combinatorial Steiner designs with two block sizes, and the related problem of finding Steiner designs with Steiner subdesigns. The later is a weaker version of the question for $(t-1)$-resolvability of a t-design that has been studied in combinatorial design theory.

Acknowledgements Research partially supported by NSA Grant H98230-06-1-0027 and NSF Grant CCR-0310632.

References

Baker RD (1976) Partitioning the planes of $AG_{2m}(2)$ into 2-designs. Discrete Math 15:205–211

Beth T, Jungnickel D, Lenz H (1999) Design theory, 2nd edn. Cambridge University Press, Cambridge

Colbourn CJ, Dinitz JF (eds) (1996) The CRC handbook of combinatorial designs. CRC, Boca Raton

Du D-Z, Hwang FK (1993) Combinatorial group testing and its applications. World Scientific, Singapore

Levenshtein VI (2003) A universal bound for a covering in regular posets and its application to pool testing. Discret Math 266:293–309

Semakov NV, Zinoviev VA, Zaitsev GV (1973) Interrelation of preparata and Hamming codes and extension of Hamming codes to new double-error-correcting codes. In: Proceedings of the 2nd international symposium on information theory, pp 257–263, Tsakhadsor, Armenia, 1971. Academiai Kiado, Budapest

Teirlinck L (1994) Some new 2-resolvable Steiner quadruple systems. Des Codes Cryptogr 4:5–10

Tonchev VD (2003) A formula for the number of Steiner quadruple systems on 2^n points of 2-rank $2^n - n$. J Comb Des 11:260–274

Tonchev VD (1996) A class of Steiner 4-wise balanced designs derived from Preparata codes. J Comb Des 3:203–204

Wilson RM (1972a) An existence theory for pairwise balanced designs, part I. J Comb Theory Ser A 13:222–245

Wilson RM (1972b) An existence theory for pairwise balanced designs, part II. J Comb Theory Ser A 13:246–273

Wilson RM (1975) An existence theory for pairwise balanced designs, part III. J Comb Theory Ser A 18:71–79