BULLETIN OF THE ICA
Volume **108** (2026), 51–68

A unified treatment of some classic combinatorial inequalities using the variance method

Douglas R. Stinson

Abstract. The "variance method" has been used to prove many classical inequalities in design theory and coding theory. The purpose of this expository note is to review and present some of these inequalities in a unified setting. I also discuss some examples from my own research where I have employed these techniques.

1 The basic idea

The "variance method" is used to prove numerous inequalities in design theory and coding theory. Essentially, we use the fact that the variance of any set of real numbers is non-negative. This underlying theme can be found in the proofs of many famous inequalities, beginning with Fisher's Inequality for BIBDs, which was proven in 1940. Most applications of the variance method begin from first principles, which is not unreasonable. However, it might be useful and instructive to discuss the technique in general. Therefore we derive some general inequalities from which many famous inequalities can be derived by "plugging in" suitable expressions depending on the application at hand.

Suppose $a_1, \ldots, a_n$ are real numbers. For $j = 0, 1, 2, \ldots$, let

$$S_j = \sum_{i=1}^{n} (a_i)^j. \tag{1}$$

Thus, $S_0 = n$, S_1 is the sum of the a_i's, etc.

Key words and phrases: BIBDs, orthogonal arrays, codes, inequalities
Mathematics Subject Classifications: 05B05, 05B15
Corresponding author: Douglas R. Stinson <dstinson@uwaterloo.ca>

Received: 28 May 2025
Accepted: 12 August 2025

Let $\bar{a}$ denote the mean of the a_i's. Then

$$\bar{a} = \frac{S_1}{n} = \frac{S_1}{S_0}.$$

It is straightforward to see that

$$0 \leq \sum_{i=1}^{n} (a_i - \bar{a})^2 = S_2 - 2\bar{a}S_1 + S_0\bar{a}^2 = S_2 - 2\frac{{S_1}^2}{S_0} + \frac{{S_1}^2}{S_0} = S_2 - \frac{{S_1}^2}{S_0}.$$

Hence, we have the following fundamental inequality.

Theorem 1.1. *Suppose that $a_1, \ldots, a_n$ are real numbers. Define S_0, S_1, and S_2 as in* (1)*. Then*

$$S_0 S_2 - {S_1}^2 \geq 0. \tag{2}$$

Remark 1.2. It is interesting to note that this exact inequality can be found in [4, p. 54]. Also, it is obvious that equality occurs in (2) if and only if $a_i = \bar{a}$ for $1 \leq i \leq n$.

In most of the applications we discuss, we start with an equation for the value

$$S^* = \sum_{i=1}^{n} \binom{a_i}{2}.$$

It is then a simple matter to compute

$$S_2 = 2S^* + S_1 \tag{3}$$

and then apply inequality (2).

An alternate derivation of inequality (2) is obtained by observing that it is just a special case of the Cauchy-Schwarz inequality. Here are a few details. The Cauchy-Schwarz inequality for real numbers states that

$$\left(\sum_{i=1}^{n} a_i b_i \right)^2 \leq \left(\sum_{i=1}^{n} {a_i}^2 \right) \left(\sum_{i=1}^{n} {b_i}^2 \right). \tag{4}$$

Let $b_1 = \cdots = b_n = 1$. Then

$$\left(\sum_{i=1}^{n} a_i \right)^2 \leq n \left(\sum_{i=1}^{n} {a_i}^2 \right). \tag{5}$$

This is equivalent to (2).

It is further known that equality occurs in (4) if and only if

$$(a_1, \ldots, a_n) = c(b_1, \ldots, b_n)$$

for some nonzero real number c. When

$$(b_1, \ldots, b_n) = (1, \ldots, 1),$$

we see that equality occurs in (5) if and only if $a_1 = \cdots = a_n$.

In some applications, we encounter situations where we have a lower bound on S_1, rather than an equality.[1] Suppose that we have equations for S_0 and S^* and suppose we know that $S_1 \geq B$, where $B > 0$. We can therefore write $S_1 = B + \epsilon$ where $\epsilon \geq 0$. We also have $S_2 = 2S^* + B + \epsilon$. Write $C = 2S^* + B$; then $S_2 = C + \epsilon$. Finally, suppose that $a_i \geq 1$ for all i. Then $S^* \geq 0$, and hence $C = 2S^* + B \geq B > 0$.

From equation (2), we have

$$S_0 \geq \frac{(B+\epsilon)^2}{C+\epsilon}.$$

Consider B and C to be fixed and define

$$f(\epsilon) = \frac{(B+\epsilon)^2}{C+\epsilon}.$$

We have

$$\begin{aligned} f'(\epsilon) &= \frac{2(C+\epsilon)(B+\epsilon) - (B+\epsilon)^2}{(C+\epsilon)^2} \\ &= \left(\frac{B+\epsilon}{(C+\epsilon)^2}\right)(2(C+\epsilon) - (B+\epsilon)) \\ &= \left(\frac{B+\epsilon}{(C+\epsilon)^2}\right)(2C - B + \epsilon). \end{aligned}$$

We noted above that $C \geq B > 0$. It follows that $2C - B + \epsilon \geq C + C - B > 0$, because $C > 0$ and $C - B \geq 0$. Therefore, $f'(\epsilon) > 0$ for all $\epsilon \geq 0$. Hence, we have that

$$S_0 \geq f(\epsilon) \geq f(0) = \frac{B^2}{C}.$$

[1] We note that a similar situation was addressed in my paper [14, Theorem 1], but the proof contained an error. Amusingly, a stronger result in the same paper had a correct proof. We also note that a correct argument was given in [15, §8.1] in the setting of the Stanton-Kalbfleisch bound.

Therefore we have proven the following.

Theorem 1.3. *Suppose that $a_1, \ldots, a_n$ are real numbers and $a_i \geq 1$ for all i. Define S_0, S_1, S_2, and S^* as in (1) and (3). Suppose further that $S_1 = B + \epsilon$ and $C = 2S^* + B$, where $B > 0$ and $\epsilon \geq 0$. Then*

$$S_0 C - B^2 \geq 0. \tag{6}$$

In the rest of this note, I derive several classical inequalities for codes and designs by applying Theorems 1.1 and 1.3. These include Fisher's inequality for BIBDs (Section 2), the Plackett-Burman bound for orthogonal arrays (Section 3), the second Johnson bound for constant-weight binary codes (Section 4), the Stanton-Kalbfleisch bound for pairwise balanced designs (Section 5), and the Mullin-Vanstone bound for (r, λ)-designs (Section 6). I also discuss a few applications and results from my own research where I have used these techniques, including the two-point sampling derandomization method (Section 7). Finally, an extension of the variance technique is briefly mentioned in Section 8.

2 Fisher's inequality

Suppose v, b, r, k, and λ are positive integers, where $v > k$. A *balanced incomplete block design* (v, b, r, k, λ)-BIBD is a collection of b *blocks*, where each block is a subset of k *points* chosen from a v-set, such that every point occurs in exactly r blocks and every pair of points occurs in exactly λ blocks. If $(X, \mathcal{A})$ is a (v, b, r, k, λ)-BIBD, then the following identities hold:

$$vr = bk, \tag{7}$$

$$\lambda(v-1) = r(k-1). \tag{8}$$

Fisher's inequality [4] states that $b \geq v$ (or, equivalently, $r \geq k$, which follows from equation (7)) in a (v, b, r, k, λ)-BIBD. Note that we require $v > k$ in an "incomplete block" design; otherwise, we could have a design with one block and $\lambda = 1$ if we allowed $v = k$.

Fisher's original proof from 1940 used the variance method. This is actually one of the more complicated ways to prove Fisher's inequality, as simpler linear algebraic proofs are found much more commonly these days in textbooks (e.g., in [15] as well as many others). However, I believe that this was the first use of the variance method to prove an inequality in combinatorial designs.

We now present a proof sketch of Fisher's original derivation of the eponymous inequality. Let $(X, \mathcal{A})$ be a (v, b, r, k, λ)-BIBD, where

$$\mathcal{A} = \{A_i : 1 \leq i \leq b\}.$$

For $1 \leq i \leq b-1$, let $a_i = |A_i \cap A_b|$. We have the following equations by simple counting:

$$S_0 = b - 1, \tag{9}$$
$$S_1 = k(r-1), \tag{10}$$
$$S^* = \tbinom{k}{2}(\lambda - 1),$$
$$S_2 = k(k-1)(\lambda-1) + k(r-1) \quad \text{from (3)}. \tag{11}$$

Now, we substitute (9), (10), and (11) into inequality (2):

$$(b-1)\big(k(k-1)(\lambda-1) + k(r-1)\big) - k^2(r-1)^2 \geq 0. \tag{12}$$

After a considerable amount of non-obvious simplification using the identities (7) and (8), the inequality (12) can be rewritten as

$$(r-k)(v-k)(r-\lambda) \geq 0. \tag{13}$$

For details, see Fisher's original paper [4].

Recall that an "incomplete block" design has $k < v$. It then follows from (8) that $\lambda < r$. Hence,

$$(v-k)(r-\lambda) > 0,$$

and therefore (13) yields the simpler inequality $r - k \geq 0$. This completes the proof of Fisher's inequality.

We see further that, in a BIBD with $v = k$, every pair of blocks intersects in exactly $\bar{a} = S_1/S_0$ points. However, if $v = b$, then $\lambda(v-1) = k(k-1)$ from (8) and

$$\bar{a} = \frac{k(r-1)}{b-1} = \frac{k(k-1)}{v-1} = \lambda.$$

So every pair of blocks intersects in exactly λ points.

Mann's inequality [7] (proven in 1969) is another inequality on the parameters of a BIBD. It states that $b \geq sv$ if there is a block that occurs with multiplicity s. The proof from [7] also uses the variance method; it is very similar to the proof of Fisher's inequality given in [4].

3 Plackett-Burman bound

Let $k \geq 2$, $n \geq 2$, and $\lambda \geq 1$ be integers. An *orthogonal array* $\mathrm{OA}_\lambda(k, n)$ is a λn^2 by k array, A, with entries from a set X of cardinality n such that, within any two columns of A, every ordered pair of symbols from X occurs in exactly λ rows. There are λn^2 rows in the OA, and every symbol occurs in exactly λn rows within each column of A.

We use the variance method to give a simple combinatorial proof of the classical Plackett-Burman bound[2] from 1946. In comparison with the proof of Fisher's inequality given in Section 2, all the remaining proofs in this paper (more precisely, the simplifications of the main inequality) are very simple.

Theorem 3.1 (Plackett-Burman bound [9, p. 310])**.** *Let $k \geq 2$, $n \geq 2$, and $\lambda \geq 1$ be integers. If there is an $\mathrm{OA}_\lambda(k, n)$, then*

$$\lambda \geq \frac{k(n-1)+1}{n^2}.$$

Proof. Relabel the symbols in each column of the OA so the last row of A is $1\,1\,\cdots\,1$. For $1 \leq i \leq \lambda n^2 - 1$, let a_i denote the number of 1's in row i of A. Then we have the following:

$$\begin{aligned}
S_0 &= \lambda n^2 - 1,\\
S_1 &= k(\lambda n - 1),\\
S^* &= \tbinom{k}{2}(\lambda - 1),\\
S_2 &= k(k-1)(\lambda-1) + k(\lambda n - 1) \quad \text{from (3)}\\
&= k\big(k(\lambda-1) + \lambda(n-1)\big).
\end{aligned}$$

Applying inequality (2), we obtain

$$(\lambda n^2 - 1)(k(k(\lambda-1) + \lambda(n-1))) \geq (k(\lambda n - 1))^2.$$

Therefore,

$$k(\lambda n - 1)^2 \leq (\lambda n^2 - 1)(k(\lambda - 1) + \lambda(n-1)).$$

[2]The Plackett-Burman bound is a special case of the better-known Rao bound [10], which was proven in 1947. The Rao bound also applies to orthogonal arrays of strength greater than two.

This simplifies to yield

$$k \leq \frac{\lambda n^2 - 1}{n - 1}.$$

Equivalently,

$$\lambda \geq \frac{k(n-1)+1}{n^2}. \qquad \square$$

The following result is proven in [3,17] using a very similar method.

Theorem 3.2. *Let $k \geq 2$, $n \geq 2$, and $\lambda \geq 1$ be integers. If there is an $\mathrm{OA}_\lambda(k, n)$ containing a row that is repeated m times, then*

$$\lambda \geq \frac{m(k(n-1)+1)}{n^2}.$$

4 The second Johnson bound

The second Johnson bound (from 1962) for constant-weight binary codes (see [6, Theorem 3]) is also proven using the variance method. As was done in [6], we first prove a result that applies to certain 0-1 matrices.

Theorem 4.1. *Suppose $A = (a_{i,j})$ is an m by n 0-1 matrix such that*

1. *every row of A has weight r,*
2. *the inner product of any two rows of A is at most λ, where $r > \lambda$.*

Then

$$m \leq \frac{n(r-\lambda)}{r^2 - n\lambda}, \tag{14}$$

provided that $r^2 - n\lambda > 0$.

Proof. For $1 \leq i \leq n$, define a_i to be the weight of column i of A. It is clear that

$$\begin{aligned} S_0 &= n, \\ S_1 &= mr. \end{aligned} \tag{15}$$

To compute S_2, we compute the number of triples in the set

$$\mathcal{T} = \big\{(i,j,k) : j < k,\ a_{j,i} = a_{k,i} = 1\big\}.$$

For a fixed value of i, there are $\binom{a_i}{2}$ triples $(i,j,k) \in \mathcal{T}$; hence,

$$|\mathcal{T}| = \sum_{i=1}^{n} \tbinom{a_i}{2}. \tag{16}$$

On the other hand, if we fix j and $k > j$, there are at most λ triples $(i, j, k) \in \mathcal{T}$; hence,

$$|\mathcal{T}| \leq \tbinom{m}{2}\lambda. \tag{17}$$

Combining (16) and (17), we obtain

$$S^* = \sum_{i=1}^{n} \tbinom{a_i}{2} \leq \tbinom{m}{2}\lambda. \tag{18}$$

We convert (18) to an equality by writing

$$S^* = \tbinom{m}{2}\lambda - \tfrac{\epsilon}{2}, \tag{19}$$

where $\epsilon \geq 0$. Here, it turns out that we can ignore ϵ without doing any extra work.

From (19) and (15), we have

$$S_2 = m(m-1)\lambda + mr - \epsilon.$$

As usual, we now apply (2). We have

$$n\big(m(m-1)\lambda + mr - \epsilon\big) \geq (mr)^2.$$

Because $\epsilon \geq 0$, we get

$$\begin{aligned} n\big(m(m-1)\lambda + mr\big) &\geq (mr)^2 \\ n\big((m-1)\lambda + r\big) &\geq mr^2 \\ m(r^2 - n\lambda) &\leq n(r-\lambda) \\ m &\leq \frac{n(r-\lambda)}{r^2 - n\lambda} \quad \text{provided that } r^2 - n\lambda > 0. \end{aligned}$$

This completes the proof. □

An $[n, r, d]$ *constant weight binary code* is a set $\mathcal{C}$ of binary vectors (codewords), each having weight r, such that the distance between any two distinct codewords is at least $d > 0$. If the inner product of two distinct codewords is λ, then the distance between the two codewords is $d = 2(r-\lambda)$. Since this quantity is even, we typically write $d = 2\delta$, where $\delta = r - \lambda > 0$ is an integer. We now apply Theorem 4.1.

Corollary 4.2. *Suppose that $\mathcal{C}$ is an $[n, r, d]$ constant weight binary code with $r > \delta = d/2 > 0$. Then*

$$|\mathcal{C}| \leq \frac{n\delta}{r^2 - n(r-\delta)},$$

provided that $r^2 - n(r-\delta) > 0$.

Proof. Apply inequality (14) with $\lambda = r - \delta$. Then

$$|\mathcal{C}| \leq \frac{n(r-(r-\delta))}{r^2 - n(r-\delta)} = \frac{n\delta}{r^2 - n(r-\delta)}. \qquad \square$$

Remark 4.3. It is interesting to observe that the Plackett-Burman bound can be derived easily as a corollary of the second Johnson bound. See [17, §3.1].

5 The Stanton-Kalbfleisch bound

In a *pairwise balanced design* (or *PBD*), we have a collection of blocks $\mathcal{A}$ (each having size at least two) in which every pair of points from a given set X occurs in a unique block. Unlike a BIBD, the blocks in a PBD may be of different sizes. We now state and prove a well-known bound on the number of blocks in a PBD that contains at least one block of a specified size k. This bound was proven by Stanton and Kalbfleisch [13] in 1972.

Theorem 5.1 (Stanton-Kalbfleisch bound, [13])**.** *Let k and v be integers such that $2 \leq k < v$. Suppose there is a PBD on v points in which there exists a block containing exactly k points. Then*

$$b \geq 1 + \frac{k^2(v-k)}{v-1}. \tag{20}$$

Proof. Suppose that $(X, \mathcal{A})$ is a PBD with $|X| = v$ such that $A \in \mathcal{A}$ is a block containing exactly k points. Denote the blocks in $\mathcal{A}$ by $A_1, \ldots, A_b$, where $A_b = A$.

Now construct a set system $(Y, \mathcal{B})$ by deleting all the points in the block A_b as follows:

$$\begin{aligned} Y &= X \backslash A_b, \\ B_i &= A_i \backslash A_b, \quad 1 \leq i \leq b-1, \quad \text{and} \\ \mathcal{B} &= \{B_i : 1 \leq i \leq b-1\}. \end{aligned}$$

Then, $(Y, \mathcal{B})$ is a set system with $v - k$ points and $b - 1$ blocks in which every pair of points occurs in a unique block. (This set system may contain blocks of size one, in which case it would technically not be a PBD.)

For $1 \leq i \leq b-1$, denote $a_i = |B_i|$. Note that $a_i = |A_i|$ or $a_i = |A_i| - 1$ for $1 \leq i \leq b-1$. Furthermore, $a_i = |A_i| - 1$ if and only if A_i intersects A_b in a point.

Denote the points in Y by y_j, $1 \le j \le v-k$. For $1 \le j \le v-k$, define

$$r_j = \big|\{B_i \in \mathcal{B} : y_j \in B_i\}\big|.$$

Then it is clear that

$$\sum_{i=1}^{b-1} a_i = \sum_{j=1}^{v-k} r_j. \tag{21}$$

Now, in the pairwise balanced design $(X, \mathcal{A})$, every point y_j must occur in a unique block with each of the points in A_b. Hence $r_j \ge k$ for all j, $1 \le j \le v-k$. Substituting into (21), it follows that

$$S_1 = \sum_{i=1}^{b-1} a_i \ge k(v-k).$$

So we have a lower bound on S_1, which is the scenario that we discussed in Theorem 1.3.

Every pair of points in Y occurs in exactly one of the B_i's, so it follows that

$$S^* = \sum_{i=1}^{b-1} \tbinom{a_i}{2} = \tbinom{v-k}{2}.$$

Thus we obtain the following three equations involving $a_1, \ldots, a_{b-1}$:

$$\begin{aligned} S_0 &= b-1, \\ S_1 &= k(v-k) + \epsilon, \\ S_2 &= (v-k)(v-k-1) + k(v-k) + \epsilon \\ &= (v-k)(v-1) + \epsilon, \end{aligned}$$

where $\epsilon \ge 0$.

We can apply equation (6) from Theorem 1.3, and it follows that

$$(b-1)(v-k)(v-1) \ge \big(k(v-k)\big)^2.$$

This simplifies to yield inequality (20). □

If equality occurs in the Stanton-Kalbfleisch bound, then every block (other than the block of size k) intersects the block of size k in a point, and every such block has exactly

$$1 + \frac{k(v-k)}{b-1} = 1 + \frac{k(v-k)(v-1)}{k^2(v-k)} = 1 + \frac{v-1}{k}$$

points.

Remark 5.2. The Stanton-Kalbfleisch bound, as presented in [13], is more general than the result given in Theorem 5.1. The general bound (which we have not stated) actually applies to μ-wise balanced designs for any $\mu \geq 2$. Here, we are only discussing the special case $\mu = 2$.

The classic Erdős-de Bruijn theorem (see [1]) states that $b \geq v$ in a PBD, and $b = v$ if and only if the PBD is a projective plane or a near-pencil. Ralph Stanton observed in his papers (e.g., [12]) that the Erdős-de Bruijn Theorem is a corollary of the Stanton-Kalbfleisch bound. The Stanton-Kalbfleisch bound asserts that $b \geq 1 + k^2(v-k)/(v-1)$. Using this fact, we compute the following:

$$\begin{aligned} b - v \geq 1 + \frac{k^2(v-k)}{v-1} - v &= \frac{k^2(v-k) - (v-1)^2}{v-1} \\ &= \frac{-v^2 + v(k^2+2) - (k^3+1)}{v-1} \\ &= \frac{-(v-(k+1))(v-(k^2-k+1))}{v-1}. \end{aligned} \tag{22}$$

Now suppose that $k+1 \leq v \leq k^2 - k + 1$. Then

$$\big(v-(k+1)\big)\big(v-(k^2-k+1)\big) \leq 0.$$

From inequality (22), we see that $b \geq v$.

If $b = v$, then one of the following two situations occurs:

1. $v = k^2 - k + 1$, every block intersects the block of size k in a point, and every block has exactly $1 + (v-1)/k = k$ points. This PBD is therefore a projective plane of order $k-1$.
2. $v = k + 1$, every block intersects the block of size k in a point, and every block (other than the block of size k) has size $1 + (v-1)/k = 2$. This PBD is a near-pencil.

6 The Mullin-Vanstone bound and an application

An (r, λ)-*design* is a PBD of index λ (i.e., every pair of points occurs in exactly λ blocks) where every point occurs in exactly r blocks. However, unlike a "normal" PBD, blocks of size 1 are allowed. We next discuss the Mullin-Vanstone bound [8], which was proven in 1975.

Theorem 6.1 (Mullin and Vanstone [8])**.** *In any (r, λ)-design on v points and b blocks, it holds that*

$$b \geq \frac{r^2 v}{r + \lambda(v-1)}.$$

The proof follows immediately from inequality (2) and the following easily derived equations:

$$\begin{aligned} S_0 &= b, \\ S_1 &= vr, \\ S^* &= \lambda\tbinom{v}{2}, \\ S_2 &= v\big(r + \lambda(v-1)\big). \end{aligned}$$

In 2011, Douglas West asked me for a bound on the largest value of s such that there exists s points and s nonincident blocks in a projective plane of order q. This question can be answered using the following corollary of the Mullin-Vanstone bound.

Corollary 6.2 (Stinson [16])**.** *If there exists a nonincident set of s points and t lines in a projective plane of order q, then*

$$t \leq \frac{q^3 + q^2 + q - qs}{q + s}. \tag{23}$$

Proof. A projective plane of order q is a $(q+1, 1)$-design on q^2+q+1 points. Suppose we choose any subset Y of s points in this projective plane. If we intersect each line (block) with Y, then we obtain a $(q+1, 1)$-design on s points. Applying Theorem 6.1, we see that the number of blocks b in this induced design satisfies the inequality

$$b \geq \frac{(q+1)^2 s}{q + s}.$$

Hence, if there are t blocks in the projective plane that are disjoint from Y, then

$$t \leq q^2 + q + 1 - \frac{(q+1)^2 s}{q+s} = \frac{q^3 + q^2 + q - qs}{q+s}. \qquad \square$$

West's question concerned the special case where $t = s$ (this corresponds to an s by s submatrix of 0's in the incidence matrix of the projective plane). If we set $s = t$ in (23), then it follows that

$$s \leq 1 + (q+1)(\sqrt{q} - 1). \tag{24}$$

As shown in [16] it is possible to attain equality in (24) if and only if the s points comprise a maximal $(s, \sqrt{q})$-arc in the projective plane. Such maximal arcs exist when q is an even power of two; they are known as Denniston arcs.

7 Two-point sampling

Chor and Goldreich [2] and (independently) Spencer [11] introduced the *two-point sampling* derandomization technique and computed error probabilities of the respective generators. In 1996, Gopalakrishan and Stinson [5] observed that these two generators could be unified and generalized by describing them in terms of orthogonal arrays, and the error analysis given in [2, 11] can be improved using the variance technique.

Here is the setting for two-point sampling. Suppose we use an $\mathrm{OA}_1(k, n)$, say A, for derandomization. There are n^2 rows in A, so a random row of A can be chosen using $2\log_2 n$ random bits. Once a random row is chosen, we run a Monte Carlo algorithm, say $\mathbf{A}$, k times, using the k elements in the chosen row as randomness for algorithm $\mathbf{A}$. Thus the number of random bits is reduced from $k\log_2 n$ (which is what would be required for k random choices) to $2\log_2 n$. However, the error probability is increased.

We present the analysis of the error probability of two-point sampling given in [5]. Suppose for the purposes of discussion that algorithm $\mathbf{A}$ is yes-biased with error probability ϵ. If I is a no-instance, then $\mathbf{A}(I)$ always returns "no." However, if I is a yes-instance, then $\mathbf{A}(I)$ can erroneously return "no" with probability ϵ. More precisely, for a yes-instance I, the number of values x such that $\mathbf{A}(I, x)$ returns "no" is ϵn. We call these *bad points* and denote the set of bad points by Y. Points that are not bad are *good points*; denote the set of good points by Z. Let $|Z| = z$; then $z = n(1 - \epsilon)$.

For a given instance I, we choose a row r of the orthogonal array A. Suppose row r contains the symbols $x_1, \ldots, x_k$. Then, we run the algorithm $\mathbf{A}(I, x_i)$ for $1 \le i \le k$ (so we run the algorithm k times, with randomness specified by the points in row r of A). For a yes-instance I, we want an upper bound on the probability that $x_1, \ldots, x_k$ are all bad points.

For a given row i, define $b_i = \left|\{j : a_{i,j} \in Z\}\right|$ (i.e., b_i is the number of good points in row i of A). Suppose there are N rows with $b_i \ge 1$, say (without loss of generality) rows $1, \ldots, N$. These are the rows that would allow us to conclude correctly that I is a yes-instance. We have the following equations

involving the values $b_1, \ldots, b_N$.

$$\begin{aligned} S_0 &= N, \\ S_1 &= knz, \\ S^* &= \tbinom{k}{2} z^2, \\ S_2 &= k(k-1)z^2 + knz = kz\big((k-1)z + n\big). \end{aligned}$$

Now we apply inequality (2):

$$\begin{aligned} Nkz\big((k-1)z+n\big) &\geq (knz)^2 \\ N\big((k-1)z+n\big) &\geq n^2 kz \\ N &\geq \frac{n^2 kz}{(k-1)z+n}. \end{aligned}$$

The number of bad rows is

$$n^2 - N \leq n^2 - \frac{n^2 kz}{(k-1)z+n} = n^2\left(1 - \frac{kz}{(k-1)z+n}\right).$$

Hence the error probability of two-point sampling is at most

$$1 - \frac{kz}{(k-1)z+n}.$$

However, $z = n(1-\epsilon)$. Hence, the error probability is at most

$$\begin{aligned} 1 - \frac{kn(1-\epsilon)}{(k-1)n(1-\epsilon)+n} &= 1 - \frac{k(1-\epsilon)}{(k-1)(1-\epsilon)+1} \\ &= \frac{\epsilon}{(k-1)(1-\epsilon)+1}. \end{aligned}$$

8 An extension of the variance method

So far, we have discussed the simplest version of the variance method. Extensions are possible, some of which lead to strengthened bounds. Recall that the fundamental idea of the variance method is that a sum of the form

$$\sum_{i=1}^{n} (a_i - \bar{a})^2$$

is non-negative for any set of real numbers $a_1, \ldots, a_n$. A related approach is based on observation that

$$\sum_{i=1}^{n} (a_i - \ell)(a_i - \ell - 1) \geq 0 \tag{25}$$

provided that the a_i's are all integers and ℓ is an integer. Further, equality holds in (25) if and only if $a_i \in \{\ell, \ell+1\}$ for all i. In any given situation, it is usually straightforward to determine the integer ℓ that leads to the strongest bound in (25). We briefly discuss a couple of examples to illustrate.

I used this approach in [14] to improve the Stanton-Kalbfleisch bound.

Theorem 8.1 (Stinson bound [14])**.** *Let k and v be integers such that $2 \leq k < v$. Suppose there is a PBD on v points in which there exists a block containing exactly k points. Then for any integer ℓ, we have*

$$b \geq 1 + \frac{(2\ell k - v + k + 1)(v - k)}{\ell^2 + \ell}. \tag{26}$$

Proof. We use the values of S_0, S_1, S_2, and S^* derived in the proof of Theorem 5.1, along with (3) and (25):

$$\begin{aligned}
0 &\leq \sum_{i=1}^{n} (a_i - \ell)(a_i - \ell - 1) \\
&= S_2 - (2\ell + 1)S_1 + (\ell^2 + \ell)S_0 \\
&= 2S^* - 2\ell S_1 + (\ell^2 + \ell)S_0 \\
&\leq (v - k)(v - k - 1) - 2\ell k(v - k) + (\ell^2 + \ell)(b - 1) \\
&= (v - k)(v - k - 1 - 2\ell k) + (\ell^2 + \ell)(b - 1) \\
b - 1 &\geq \frac{(v - k)\big(2\ell k - (v - k - 1)\big)}{\ell^2 + \ell} \\
b &\geq 1 + \frac{(2\ell k - v + k + 1)(v - k)}{\ell^2 + \ell}.
\end{aligned}$$

□

The strongest application of Theorem 8.1 is obtained by taking

$$\ell = \left\lfloor \frac{v - 1}{k} \right\rfloor.$$

For this particular choice of ℓ, the lower bound given in Theorem 8.1 is always greater than or equal to the Stanton-Kalbfleish bound; see [14] for details.

A similar method is used by Johnson [6] in order to provide an improvement of Theorem 4.1. We use the values of S_0, S_1, S_2, and S^* derived in the proof

of Theorem 4.1, along with (3) and (25). The following is obtained:

$$\begin{aligned} 0 &\le 2S^* - 2\ell S_1 + (\ell^2+\ell)S_0 \quad \text{as in the proof of Theorem 8.1} \\ &\le \lambda m(m-1) - 2\ell mr + (\ell^2+\ell)n \end{aligned}$$

$$m(m-1)\lambda \ge 2\ell mr - (\ell^2+\ell)n. \tag{27}$$

Following Johnson [6], we take $\ell = \lfloor mr/n \rfloor$, and we write

$$mr = n\ell + t, \tag{28}$$

where $0 \le t \le n-1$. For this value of ℓ, the inequality (27) can be rewritten as follows:

$$\begin{aligned} m(m-1)\lambda &\ge 2\ell(n\ell+t) - (\ell^2+\ell)n \quad \text{from (28)} \\ &= 2\ell^2 n + 2\ell t - \ell^2 n - \ell n \\ &= \ell^2 n + 2\ell t - \ell n \\ &= \ell^2 n + 2\ell t - (mr - t) \quad \text{from (28)} \\ &= \ell^2 n + 2\ell t + t - mr \\ &= \ell^2 n - \ell^2 t + \ell^2 t + 2\ell t + t - mr \\ &= (n-t)\ell^2 + t(\ell+1)^2 - mr. \end{aligned}$$

We have proven the following.

Theorem 8.2 (Johnson [6, eq. (6)])**.** *Suppose $A = (a_{i,j})$ is an m by n 0-1 matrix such that*

1. *every row of A has weight r,*
2. *the inner product of any two rows of A is at most λ, where $r > \lambda$.*

Let $\ell = \lfloor mr/n \rfloor$ and write $mr = n\ell + t$, where $0 \le t \le n-1$. Then

$$m(m-1)\lambda \ge (n-t)\ell^2 + t(\ell+1)^2 - mr. \tag{29}$$

If we regard n, r, and λ as being fixed, we would then compute the largest integer m that satisfies (29). Of course, this is just a necessary condition for the existence of the desired 0-1 matrix.

Acknowledgment

This research was supported by an NSERC General Research Funds grant (University of Waterloo).

References

[1] N. G. de Bruijn and P. Erdős, On a combinatorial problem, *Indagationes Math.* **10** (1948), 421–423.

[2] B. Chor and O. Goldreich, On the power of two-point based sampling, *J. Complexity* **5** (1989), 96–106.

[3] C. J. Colbourn, D. R. Stinson, and S. Veitch, Constructions of optimal orthogonal arrays with repeated rows, *Discrete Math.* **342** (2019), 2455–2466.

[4] R. A. Fisher, An examination of the different possible solutions of a problem in incomplete blocks, *Ann. Eugenics* **10** (1940), 52–75.

[5] K. Gopalakrishnan and D. R. Stinson, A simple analysis of the error probability of two-point based sampling, *Inform. Process. Lett.* **60** (1996), 91–96.

[6] S. M. Johnson, A new upper bound for error-correcting codes, *IRE Trans. on Inform. Theory* **8** (1962), 203–207.

[7] H. B. Mann, A note on balanced incomplete-block designs, *Ann. Math. Statist.* **40** (1969), 679–680.

[8] R. C. Mullin and S. A.Vanstone, On regular pairwise balanced designs of order 6 and index 1, *Util. Math.* **8** (1975), 349–369.

[9] R. L. Plackett and J. P. Burman, The design of optimum multifactorial experiments, *Biometrika* **33** (1946), 305–325.

[10] C. R. Rao, Factorial experiments derivable from combinatorial arrangements of arrays, *Suppl. J. Roy. Statist. Soc.* **9** (1947), 128–139.

[11] T. H. Spencer, Provably good pattern generators for a random pattern test, *Algorithmica* **11** (1994), 429–442.

[12] R. G. Stanton, P. Eades, J. van Rees, and D. D. Cowan, Computation of some exact g-coverings, *Util. Math.* **18** (1980), 269–282.

[13] R. G. Stanton and J. G. Kalbfleisch, The λ-μ problem: $\lambda = 1$ and $\mu = 3$, In "Proc. Second Chapel Hill Conf. on Combinatorics" (1972), pp. 451–462.

[14] D. R. Stinson, Applications and generalizations of the variance method in combinatorial designs, *Util. Math.* **22** (1982), 323–333.

[15] D. R. Stinson, *Combinatorial designs: Constructions and analysis*, Springer-Verlag, New York, 2004.

[16] D. R. Stinson, Nonincident points and blocks in designs, *Discrete Math.* **313** (2013), 447–452.

[17] D. R. Stinson, Bounds for orthogonal arrays with repeated rows, *Bull. Inst. Combin. Appl.* **85** (2019), 60–73.

Douglas R. Stinson
David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
dstinson@uwaterloo.ca
0000-0001-5635-8122