Some results on weighing matrices

Jennifer Seberry Wallis and Albert Leon Whiteman

It is shown that if \( q \) is a prime power then there exists a circulant weighing matrix of order \( q^2 + q + 1 \) with \( q^2 \) non-zero elements per row and column.

This result allows the bound \( N \) to be lowered in the theorem of Geramita and Wallis that "given a square integer \( k \) there exists an integer \( N \) dependent on \( k \) such that weighing matrices of weight \( k \) and order \( n \) and orthogonal designs \((l, k)\) of order \( 2n \) exist for every \( n > N \)."

1. Introduction

An orthogonal design of order \( n \) and type \((s_1, s_2, \ldots, s_l)\) \((s_i > 0)\) on the commuting variables \( x_1, x_2, \ldots, x_l \) is an \( n \times n \) matrix \( A \) with entries from \( \{0, \pm x_1, \ldots, \pm x_l\} \) such that

\[
AA^t = \left[ \sum_{i=1}^{l} s_i x_i^2 \right] I_n.
\]

Alternatively, the rows of \( A \) are formally orthogonal and each row has precisely \( s_i \) entries of the type \( \pm x_i \).

In [2], where this was first defined and many examples and properties of such designs were investigated, it is mentioned that

\[
A^t A = \left[ \sum_{i=1}^{l} s_i x_i^2 \right] I_n
\]

and so the alternative description of \( A \) applies equally well to the

Received 17 February 1975.

433
columns of \( A \). It is also shown in [2] that \( l \leq \rho(n) \), where \( \rho(n) \) (Radon’s function) is defined by

\[
\rho(n) = 8c + 2^d
\]

when

\[
n = 2^a \cdot b, \ b \text{ odd, } a = 4c + d, \ 0 \leq d < 4 .
\]

Also in [2] it is shown that if there is an orthogonal design of order \( n \) and type \((a^2, b)\), then

(i) \( n \equiv 2 \pmod{4} \Rightarrow b = c^2 \) for some integer \( c \),

(ii) \( n = 4t \), \( t \) odd \( \Rightarrow b \) is the sum of three integer squares;

while in [5] it is shown that if \( n \equiv 4 \pmod{8} \) and if there exists an orthogonal design of order \( n \) and type

(i) \((a, a, a, b)\), then \( \frac{b}{a} \) is a rational square;

(ii) \((a, a, b)\), then \( \frac{b}{a} \) is the sum of two rational squares;

(iii) \((a, b)\), then \( \frac{b}{a} \) is the sum of three rational squares.

A weighing matrix of weight \( k \) and order \( n \) is a square \( \{0, 1, -1\} \) matrix, \( W = W(n, k) \), of order \( n \) satisfying

\[
WW^t = kI_n .
\]

In [2] it is shown that the existence of an orthogonal design of order \( n \) and type \((s_1, \ldots, s_l)\) is equivalent to the existence of weighing matrices \( A_1, \ldots, A_l \), of order \( n \), where \( A_i \) has weight \( s_i \) and the matrices, \( \{A_i\}_{i=1}^l \), satisfy the matrix equation

\[
XY^t + YX^t = 0
\]

in pairs. In particular, the existence of an orthogonal design of order \( n \) and type \((1, k)\) is equivalent to the existence of a skew-symmetric weighing matrix of weight \( k \) and order \( n \).

It is conjectured that:
(i) for $n \equiv 2 \pmod{4}$ there is a weighing matrix of weight $k$ and order $n$ for every $k < n - 1$ which is the sum of two integer squares;

(ii) for $n \equiv 0 \pmod{4}$ there is a weighing matrix of weight $k$ and order $n$ for every $k \leq n$;

(iii) for $n \equiv 4 \pmod{8}$ there is a skew-symmetric weighing matrix of order $n$ for every $k < n$, where $k$ is the sum of at most three squares of integers (equivalently, there is an orthogonal design of type $(1,k)$ in order $n$ for every $k < n$ which is the sum of at most three squares of integers. In other words, the necessary condition for the existence of an orthogonal design of type $(1,k)$ in order $n$, $n \equiv 4 \pmod{8}$ is also sufficient);

(iv) for $n \equiv 0 \pmod{8}$ there is a skew-symmetric weighing matrix of order $n$ for every $k < n$ (equivalently there is an orthogonal design of type $(1,k)$ in order $n$ for every $k < n$);

(v) for $n \equiv 2 \pmod{4}$ there is an orthogonal design of type $(1,k)$ in order $n$ for every $k < n - 1$ such that $k$ is an integer square.

Conjecture (ii) above is an extension of the Hadamard conjecture (that is, for every $n \equiv 0 \pmod{4}$ there is a $\{1, -1\}$ matrix, $H$, of order $n$ satisfying $HH^t = nI_n$) while (iv) and (iii) generalize the conjecture that for every $n \equiv 0 \pmod{4}$ there is a Hadamard matrix, $H$, of order $n$, with the property that $H = I_n + S$ where $S = -S^t$.

Conjecture (ii) was established in [10] for $n \in \{4, 8, 12, \ldots, 32, 40\}$ and in [6] for $n = 2^t$. Conjecture (iii) was established in [3, Theorem 17] for $n = 2^t$ ($t \geq 3$).

Conjectures (iv) and (iii) (and as a consequence conjecture (ii)) were established for $n = 2^{t+1} \cdot 3$, $n = 2^{t+1} \cdot 5$, $t$ a positive integer, in [4] and in [11] for $n = 2^{t+1} \cdot 9$. Also in [3] it was shown that only
k = 46, 47 in order 56 remain to be found and the conjectures will be settled for \( n = 2^{t+1} \cdot 7 \).

It has been established [5] that given a square \( k \) there exists an \( N(k) \) such that \( W(n, k) \) exists for every \( n > N \). Consequently an orthogonal design \( (l, k) \) exists in every order \( 2n, n > N \).

Here we give some results which allow \( N(k) \) to be lowered when \( k \) has a factor of 4.

Let \( R \) be the back diagonal matrix. Then an orthogonal design or weighing matrix is said to be constructed from two circulant matrices \( A \) and \( B \) if it is of the form

\[
\begin{bmatrix}
A & BR \\
BR & -A
\end{bmatrix}
\]

and to be of Goethals-Seidel type if it is of the form

\[
\begin{bmatrix}
A & BR & CR & DR \\
-BR & A & D^t R & -C^t R \\
-CR & -D^t R & A & B^t R \\
-DR & C^t R & -B^t R & A
\end{bmatrix}
\]

where \( A, B, C, D \) are circulant matrices.

Let \( S_1, S_2, \ldots, S_n \) be subsets of \( V \), a finite abelian group, containing \( k_1, k_2, \ldots, k_n \) elements respectively. Write \( T_i \) for the totality of all differences between elements of \( S_i \) (with repetitions), and \( T \) for the totality of elements of all the \( T_i \). If \( T \) contains each non-zero element of \( V \) a fixed number of times, \( \lambda \) say, then the sets \( S_1, S_2, \ldots, S_n \) will be called \( n - \{v; k_1, k_2, \ldots, k_n; \lambda\} \) supplementary difference sets.

2. Weighing matrices of odd order

If \( A \) is a \( W(n, k) \), then \( (\det A)^2 = k^N \). Thus if \( n \) is odd and a \( W(n, k) \) exists, then \( k \) must be a perfect square.

In [2] where they are first discussed it is shown that
Weighing matrices 437

\[(n-k)^2 - (n-k) + 2 > n\]

must also hold. It is noted there that the "boundary" values of this condition are of special interest; that is, if

\[(n-k)^2 - (n-k) + 1 = n ,\]

for in this case the zeros of \( A \) occur such that the incidence between any pair of rows is exactly one. So if we let \( B = J - A^*A \), \( B \) satisfies

\[BB^t = (n-k-1)I_n + J_n , \quad BJ = (n-k)J_n ;\]

that is, \( B \) is the incidence matrix of the projective plane of order \( n - k - 1 \).

Thus, the Bruck-Ryser Theorem on the non-existence of projective planes of various orders implied the non-existence of the appropriate \( \mathcal{W}(n, k) \).

We shall prove in this paper that if \( q \) is a prime power, then a circulant weighing matrix of the form

\[\mathcal{W}(q^2+q+1, q^2)\]

can be constructed. Our method makes use of near difference sets.

In [8] Ryser has given the following definition of a near difference set.

Let \( m \geq 4 \) be an even integer, and let \( k \) and \( \lambda \) be positive integers. A near difference set

\[D = \{d_1, d_2, \ldots, d_k\}\]

is a set of \( k \) residues modulo \( m \) with the property that, for any residue \( a \neq 0 \), \( m/2 \) (mod \( m \)), the congruence

\[d_i - d_j \equiv a \pmod{m}\]

has exactly \( \lambda \) solution pairs \( (d_i, d_j) \) with \( d_i \) and \( d_j \) in \( D \) and no solution pairs for \( a \equiv m/2 \) (mod \( m \)).

A necessary condition for the existence of a near difference set with
parameters $m, k, \lambda$ is that
\[ k(k-1) = \lambda(m-2) . \]

Let us put
\[ m = 2v . \]

Then the necessary condition becomes
\[ k(k-1) = 2\lambda(v-1) . \]

Examples of near difference sets are:

(i) $v = 7, k = 4, \lambda = 1, m = 14$,
\[
\begin{array}{cccc}
0 & 1 & 4 & 6 \\
\end{array}
\]

(ii) $v = 13, k = 9, \lambda = 3, m = 26$,
\[
\begin{array}{cccccccccccc}
0 & 1 & 6 & 8 & 10 & 11 & 12 & 15 & 18 \\
\end{array}
\]

(iii) $v = 21, k = 16, \lambda = 6, m = 42$,
\[
\begin{array}{cccccccccccccccc}
0 & 1 & 10 & 11 & 18 & 20 & 23 & 25 & 26 & 29 & 30 & 34 & 36 & 37 & 38 & 40 \\
\end{array}
\]

In [7] Elliott and Butson proved that if $q$ is an odd prime power, then we can construct a near difference set with parameters
\[ m = 2(1+q+q^2), \ k = q^2, \ \lambda = \frac{1}{2}q(q-1) . \]

Spence [9] showed that the construction of Elliott and Butson is also valid when $q$ is a power of 2.

The three examples of near difference sets that we have given illustrate the cases $q = 2, 3, 4$ of the Elliott-Butson-Spence result.

Suppose that we are given a near difference set
\[ D = \{d_1, d_2, \ldots, d_k\} \]
with parameters $m, k, \lambda$. Then the polynomial
Weighing matrices

\[ \alpha(x) = \sum_{d \in D} x^d \]

is the Hall polynomial associated with \( D \). Since \( D \) is a near difference set we have

\[ \alpha(x)\alpha(x^{-1}) \equiv k + \lambda (x + x^2 + \ldots + x^{v-1} + x^{v+1} + \ldots + x^{2v-1}) \pmod{x^{2v-1}}. \]

If we write \( T_2(x) = 1 + x + x^2 + \ldots + x^{v-1} \) this takes the form

\[ \alpha(x)\alpha(x^{-1}) \equiv k + \lambda \left( T_2(x)-T_2(x^v) \right) \pmod{x^{2v-1}}. \]

In the rest of this discussion let \( D \) denote the near difference set of Elliott-Butson-Spence. The parameters of \( D \) are given by

\[ m = 2(q^2+q+1), \quad k = q^2, \quad \lambda = \frac{q(q-1)}{2}. \]

If \( \alpha(x) = \sum_{d \in D} x^d \), then we have

\[ \alpha(x)\alpha(x^{-1}) \equiv q^2 + \frac{q(q-1)}{2} (x + x^2 + \ldots + x^{v-1} + x^{v+1} + \ldots + x^{2v-1}) \pmod{x^{2v-1}}, \]

where \( v = 1 + q + q^2 \). Let \( k_1 \) be the number of odd integers in \( D \), and \( k_2 \) the number of even integers in \( D \). Since a translate of \( D \) is also a near difference set with the same parameters we may assume without loss of generality that

\[ k_2 \geq k_1. \]

For \( x = -1 \) we have

\[ \alpha(-1) = k_2 - k_1, \quad \alpha^2(-1) = q^2. \]

Hence

\[ \alpha(-1) = q. \]

The two equations

\[ -k_1 + k_2 = q, \]

\[ \alpha(-1) = q. \]
$k_1 + k_2 = q^2$,

yield

$$k_1 = \frac{q^2 - q}{2}, \quad k_2 = \frac{q^2 + q}{2}.$$ 

Let us now put

$$F(x) = \sum_{d \in D} x^d, \quad G(x) = \sum_{d \in D} x^d.$$ 

Then we have

$$\alpha(x) = F(x) + G(x),$$

$$\alpha(x^{-1}) = F(x^{-1}) + G(x^{-1}),$$

so that

$$\alpha(x)\alpha(x^{-1}) = F(x)F(x^{-1}) + G(x)G(x^{-1}) + F(x)G(x^{-1}) + F(x^{-1})G(x).$$

It is clear that

(1) \hspace{1cm} F(x)F(x^{-1}) + G(x)G(x^{-1}) \equiv \hspace{1cm}
\equiv q^2 + \frac{q(q-1)}{2} (x^2 + x^4 + \ldots + x^{2v-2}) \pmod{x^{2v-1}},

(2) \hspace{1cm} F(x)G(x^{-1}) + F(x^{-1})G(x) \equiv \hspace{1cm}
\equiv \frac{q(q-1)}{2} (x + x^3 + \ldots + x^{v-2} + x^{v+2} + \ldots + x^{2v-1}) \pmod{x^{2v-1}}.

We next put

$$\alpha_1(x) = \sum_{d \in D} x^{(d+v)/2}, \quad \alpha_2(x) = \sum_{d \in D} x^{d/2}.$$ 

Then the reduction of (1) \ mod \ x^{v-1} \ yields

(3) \hspace{1cm} \alpha_1(x)\alpha_1(x^{-1}) + \alpha_2(x)\alpha_2(x^{-1}) \equiv q^2 + \frac{q(q-1)}{2} (x + x^2 + \ldots + x^{v-1}) \pmod{x^{v-1}}.

The reduction of (2) \ mod \ x^{v-1} \ yields
We shall prove the following theorem.

**Theorem 1.** Let $q$ be a prime power. Then a circulant weighing matrix of the form

$$W(q^2+q+1, q^2)$$

can be constructed.

**Proof.** Let $D = \{d_1, d_2, \ldots, d_k\}$ be an Elliott-Butson-Spence near difference set with parameters

$$m = 2(q^2+q+1), \quad k = q^2, \quad \lambda = \frac{q(q-1)}{2}.$$ 

We again put $v = q^2 + q + 1$. Let $S$ be the set of $v$ integers: 0, 1, 2, ..., $v-1$. We partition $S$ into three subsets as follows:

$$S = T_1 \cup T_2 \cup T_3$$

where

$$T_1 = \left\{ \frac{d+v}{2} \pmod{v}, \right\}$$

$$T_2 = \left\{ \frac{d}{2} \pmod{v}, \right\}$$

$$T_3 = \{ s \in S, s \not\in T_1, s \not\in T_2 \}.$$ 

There are $k_1$ integers in $T_1$, $k_2$ integers in $T_2$, and $v - k_1 - k_2$ integers in $T_3$.

The sets $T_1$ and $T_2$ are disjoint. For if

$$\frac{d+v}{2} \equiv \frac{d}{2} \pmod{v}$$

then

$$d_i - d_j \equiv v \pmod{2v}, \quad (d_i, d_j \in D),$$

in violation of the definition of a near difference set.
The initial row
\[ a_0, a_1, \ldots, a_{v-1} \]
of the circulant \( W(q^2+q+1, q^2) \) is now constructed as follows:
\[
a_i = \begin{cases} 
-1 & \text{if } i \in T_1, \\
1 & \text{if } i \in T_2, \\
0 & \text{if } i \in T_3.
\end{cases}
\]

Define \( \psi(x) = \frac{v-1}{\ell} \sum_{i=0}^{v-1} a_i x^i \). Then we have
\[
\psi(x) = a_2(x) - a_1(x),
\]
\[
\psi(x^{-1}) = a_2(x^{-1}) - a_1(x^{-1}),
\]
so that
\[
\psi(x) \psi(x^{-1}) = a_1(x)a_1(x^{-1}) + a_2(x)a_2(x^{-1}) - a_1(x)a_2(x^{-1}) - a_1(x^{-1})a_2(x)
\]
\[
= q^2 + \frac{q(q-1)}{2} (x + x^2 + \ldots + x^{v-1}) - \frac{q(q-1)}{2} (x + x^2 + \ldots + x^{v-1})
\]
\[
= q^2 \quad \text{(mod } x^v-1)\text{).}
\]
Replacing \( x \) by \( \zeta \) (where \( \zeta^v = 1 \)) we obtain
\[
\psi(\zeta)\psi(\zeta^{-1}) = q^2.
\]
The last relation is valid for each \( v \)th root of unity \( \zeta \) including \( \zeta = 1 \). For \( \zeta = 1 \) we have
\[
\psi(1) = k_2 - k_1 = \frac{q(q+1)}{2} - \frac{q(q-1)}{2} = q.
\]
We next apply the finite Parseval relation:
\[
\frac{v-1}{\ell} \sum_{i=0}^{v-1} a_i^* a_{i+r} = \frac{1}{v} \sum_{j=0}^{v-1} |\psi(\zeta^j)|^2 \zeta^{jr}.
\]
For \( r = 0 \) we have
Weighing matrices

\[
\sum_{i=0}^{v-1} a_i^2 = \frac{1}{v} nq^2 = q^2 .
\]

For \(1 \leq r \leq v-1\) we get

\[
\sum_{i=0}^{v-1} a_i a_{i+r} = \frac{1}{v} \cdot q^2 \cdot 0 = 0 .
\]

This completes the proof of the orthogonality of the circulant \(w(q^2+q^1, q^2)\).

3. Other observations

We next note that the sets \(T_1, T_2\) constitute

\[
2 - \left\{ v; k_1, k_2; k_1 + k_2 - \frac{v-1}{2} \right\}
\]

supplementary difference sets. Since \(k_1 = \frac{q(q-1)}{2}, k_2 = \frac{q(q+1)}{2}\), we have

\[
\lambda = k_1 + k_2 - \frac{v-1}{2} = k_1 .
\]

The result follows at once from

\[
\alpha_1(x)\alpha_1(x^{-1}) + \alpha_2(x)\alpha_2(x^{-1}) \equiv q^2 + \frac{q(q-1)}{2} (x + x^2 + \ldots + x^{v-1}) \pmod{x^{v-1}} .
\]

We are now in the position to construct the Hadamard matrix, \(H_{292}\), of Spence. We use the following well-known result.

Let \(p = 2n + 1\) be a prime. Let \(U\) be the set of quadratic residues of \(p\), and \(V\) the set of quadratic non-residues of \(p\). Then \(U\) and \(V\) constitute

\[
2 - \left\{ v; k_3, k_4; k_3 + k_4 - \frac{v+1}{2} \right\}
\]

supplementary difference sets. Here we have

\[
v = p = 2n + 1 ; \quad k_3 = k_4 = n ; \quad \lambda = n - 1 .
\]

Combining our results we find that if \(v = q^2 + q + 1\) is a prime, then we construct
supplementary difference sets, and also

$$2 - \{v; k_1, k_2; k_1 + k_2 - \frac{v-1}{2}\}$$

supplementary difference sets. It follows that we have

$$4 - \{v; k_1, k_2, k_3, k_4; k_1 + k_2 + k_3 + k_4 - v\}$$

supplementary difference sets, which may be used to construct an Hadamard matrix $H_{4v}$ of Williamson type.

In particular for $q = 8$ we have $v = 73$. Therefore we can construct $H_{292}$.

Our next objective is to show that the $k_1 + k_2$ numbers in $T_1 \cup T_2$ constitute an ordinary difference set with parameters

$$v = q^2 + q + 1, \quad k = q^2, \quad \lambda = q^2 - q.$$

For this purpose we form the polynomial

$$A(x) = \alpha_1(x) + \alpha_2(x)$$

so that

$$A(x^{-1}) = \alpha_1(x^{-1}) + \alpha_2(x^{-1}).$$

Then we have

$$A(x)A(x^{-1}) = \alpha_1(x)\alpha_1(x^{-1}) + \alpha_2(x)\alpha_2(x^{-1}) + \alpha_1(x)\alpha_2(x^{-1}) + \alpha_1(x^{-1})\alpha_2(x)$$

$$\equiv q^2 + \frac{q(q-1)}{2} (x + x^2 + \ldots + x^{v-1}) + \frac{q(q-1)}{2} (x + x^2 + \ldots + x^{v-1})$$

$$(\text{mod } x^{v-1})$$

$$\equiv q^2 + q(q-1)(x + x^2 + \ldots + x^{v-1}) \pmod{x^{v-1}}.$$

The set $T_3$ is the complement of $T_1 \cup T_2$. Therefore the integers in $T_3$ constitute a difference set with parameters

$$v^* = v, \quad k^* = v - k = q + 1, \quad \lambda^* = v - 2k + \lambda = 1.$$
4. Applications to weighing matrices and orthogonal designs

The existence of the $W(21, 16)$ allows us to make the following statements.

**Theorem 2.** There exists a $W(n, 16)$ for every $n \in \{16, 18, 20, 21, 22, 24, 26, \ldots, 36\}$, and all orders $\geq 36$.

*Proof.* In [5] it was noted that a $W(n, 16)$ exists for $n \in \{16, 18, 20, \ldots, 64\}$, and all orders $\geq 64$. Thus the existence of a $W(21, 16)$ allows this set to be replaced by that of the enunciation.

**Theorem 3.** There exist orthogonal designs $(1, 9)$ and $(1, 16)$ in every order $2^n$, $n \geq 21$.

*Proof.* These results follow using the $W(21, 16)$ to obtain a $(1, 16)$ in order $42$ and then noting from Tables 1 and 2 of [4] that each order $2^n$, $n \geq 21$ can be written as $2m_1 + 2m_2$ where $(1, 9)$ and $(1, 16)$ exist for both orders $2m_1$ and $2m_2$.

**Theorem 4.** There exists a $W(42, a^2+b^2)$ for integers $a, b$ except possibly for $a^2 + b^2 \in \{18, 25, 29, 36, 37\}$.

*Proof.* Since a $W(22, k)$ and $W(20, k)$ exist for $k \in \{a^2+b^2 : a^2+b^2 \leq 20, a^2+b^2 \neq 18\}$ [4; Table 2] we have $W(42, k) = W(22, k) \oplus W(20, k)$ for the same $k$.

There is a $W(42, k)$ for $k \in \{26, 32, 40\}$ by [4; Proposition 13]. Writing $A = W(21, 16)$ we see

$$
\begin{bmatrix}
A+I & A-I \\
A^{t}-I & -A^{t}-I
\end{bmatrix}
$$

is a $W(42, 34)$. Finally since $41$ is a prime the construction of Goethals and Seidel [7] gives a $W(42, 41)$ and we have the result.

**Theorem 5.** Since there exists a $W = W(q^2+q+1, q^2)$ for every prime power $q$ there exist orthogonal designs

(i) $(1, q^2)$ and $(q^2, q^2)$ in order $2(q^2+q+1)$;
(ii) \((1, 1, 1, q^2), (1, 1, q^2, q^2), (1, q^2, q^2, q^2), \)
\((q^2, q^2, q^2, q^2), (1, 4, q^2), (1, 1, 2(q^2+1)), \)
\((1, q^2, 2(q^2+1)), (q^2, q^2, 2(q^2+1)), (2(q^2+1), 2(q^2+1))\)
in every order \(4(q^2+q+1)\);

(iii) \((1, 1, 2, q^2, q^2, q^2)\) (at least) in every order
\(8(q^2+q+1)\);

(iv) \((2q^2, 2(q^2+2q+2))\) in order \(4(q^2+q+1)\) with \(q^2 + q + 1\)
a prime.

Proof. Use \(I, W\) in various combinations in the Geothals-Seidel
array for (i), (ii), (iii).

For (iv) we note that \(W^*A = 0\) where \(A\) is the incidence matrix of
the \((q^2+q+1, q+1, 1)\) configuration satisfying
\[AA^t = qI + J\]
and \(*\) is the Hadamard product. For every prime order, \(p\), there exist
circulant matrices \(X, Y\) satisfying
\[XX^t + YY^t = 2(p+1)I - 2J.\]

Then
\[aW+bA, aW-bA, bX, bY\]
may be used in the Goethals-Seidel array to give the required result.

**THEOREM 6.** Since there exists a \(W(q^2+q+1, q^2)\) for every prime
power \(q\) there exist

(i) \(W(2(q^2+q+1), 2(q^2+1))\);

(ii) \(W(q^2+q+1, 4(q^2+2))\).

**References**

J. Math.* 10 (1966), 517-531.


Department of Mathematics, Institute of Advanced Studies, Australian National University, Canberra, ACT.

Department of Mathematics, University of Southern California, Los Angeles, California, USA.