# Many More Names of (7, 3, 1)

EZRA BROWN
Virginia Polytechnic Institute and State University
Blacksburg, VA 24061-0123
ezbrown@math.vt.edu

Combinatorial designs are collections of subsets of a finite set that satisfy specified conditions, usually involving regularity or symmetry. As the scope of the 984-page *Handbook of Combinatorial Designs* [**7**] suggests, this field of study is vast and far reaching. Here is a picture of the very first design to appear in "Opening the Door," the first of the *Handbook*'s 109 chapters:

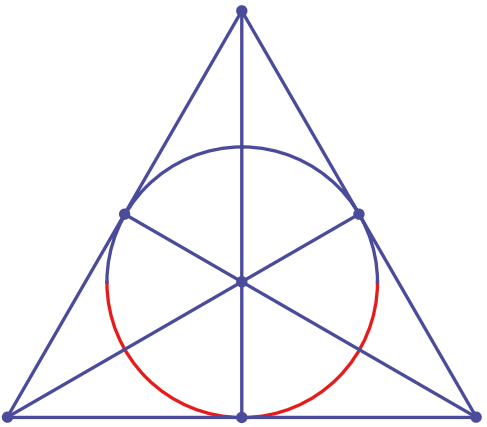

**Figure 1** The design that opens the door

This design, which we call the (7, 3, 1) design, makes appearances in many areas of mathematics. It seems to turn up again and again in unexpected places. An earlier paper in this MAGAZINE [**4**] described (7, 3, 1)'s appearance in a number of different areas, including finite projective planes, as the Fano plane (FIGURE 1); graph theory, as the Heawood graph and the doubly regular round-robin tournament of order 7; topology, as an arrangement of six mutually adjacent hexagons on the torus; $(-1, 1)$ matrices, as a skew-Hadamard matrix of order 8; and algebraic number theory, as the splitting field of the polynomial $(x^2 - 2)(x^2 - 3)(x^2 - 5)$.

In this paper, we show how (7, 3, 1) makes appearances in three areas, namely (1) Hamming's error-correcting codes, (2) Singer designs and difference sets based on $n$-dimensional finite projective geometries, and (3) normed algebras.

We begin with an overview of block designs, including two descriptions of (7, 3, 1). We then describe certain binary error-correcting codes called Hamming codes, in which (7, 3, 1) makes three different appearances. Next, we expand the treatment of Hamming codes from binary codes to codes over all finite fields $\mathbb{F}_q$, where $q$ is an odd prime. Then, we describe generalizations of the block design structure of (7, 3, 1) to

*Math. Mag.* **88** (2015) 103–120. doi:10.4169/math.mag.88.2.103. 
MSC: Primary 05B05, Secondary 11R52; 17A35; 94B05.

the so-called Singer designs in the finite projective geometries $PG(n, q)$, as well as the Singer difference sets associated with these designs.

We continue with a fascinating connection between (7, 3, 1) and two number systems—the real algebras of dimensions 8 and 16, called the octonions and the sedenions, respectively. These superficially resemble the complex numbers, and mathematicians were led to these systems by asking questions about sums of squares. It turns out that (7, 3, 1) has two distinct connections with the octonions and makes 15 appearances within the sedenions.

But first, let's talk about block designs in general and (7, 3, 1) in particular.

## Block designs

Let $v, b, r, k,$ and $\lambda$ be positive integers, with $v > k$. A *balanced incomplete block design* (or BIBD) with parameters $v, b, r, k,$ and $\lambda$ is an collection of $b$ subsets (or *blocks*) of a $v$-element set $V$ of elements such that each block contains $k$ points, each element in $V$ appears in exactly $r$ blocks, and each pair of elements appears together in exactly $\lambda$ blocks.

The parameters are not independent, for they satisfy the two equalities $bk = vr$ and $r(k-1) = \lambda(v-1)$; let's see why this is so. First, there are two ways to count the number of pairs $\{B, x\}$ such that the block $B$ contains the element $x$. Each of the $b$ blocks contains $k$ elements, making $bk$ pairs in all, and each of the $v$ elements appears in $r$ blocks, making $vr$ pairs in all. It follows that

$$bk = vr.$$

Next, fix an element $x$. There are two ways to count the number of pairs $\{B, y\}$ such that $x$ and $y$ appear together in a block $B$. The element $x$ is contained in $r$ blocks, and each such block contains $k-1$ other elements; also, the element $x$ appears with another element $y$ in $\lambda$ blocks, and there are $v-1$ elements $y \neq x$ in all. It follows that

$$r(k-1) = \lambda(v-1).$$

Thus, the parameters $v, k$ and $\lambda$ are enough to specify a block design and so we may speak of a $(v, k, \lambda)$ design.

The two equalities are necessary for the existence of a BIBD with the given parameters. Clearly, there cannot be a $(v, k, \lambda)$ design if $r$ and $b$ are not integers. But even if $r$ and $b$ are integers and the two equalities are satisfied, it happens that some combinations of parameters $(v, k, \lambda)$ do not describe any designs. There are deep reasons that, for example, no designs with parameters (22, 7, 2) and (43, 7, 1) exist.

A BIBD is called *symmetric* if $v = b$, and so $r = k$; in this paper, *all of the designs we will consider are symmetric*. A (7, 3, 1) design consists of seven three-element subsets of $V = \{1, 2, 3, 4, 5, 6, 7\}$ such that each element is in three blocks and each pair of elements is together in a unique block. Since $v = b = 7$ and $r = k = 3$, this design is symmetric, and we can describe its blocks in two ways: (a) as $\mathcal{D}$, the seven translates mod 7 of the triple $D_1 = \{1, 2, 4\}$, and (b) as $\mathcal{H}$, the triples $\{1, 2, 3\}$, $\{1, 4, 5\}$, $\{1, 6, 7\}$, $\{2, 4, 6\}$, $\{2, 5, 7\}$, $\{3, 4, 7\}$, and $\{3, 5, 6\}$. FIGURE 2 shows both $\mathcal{D}$ and $\mathcal{H}$.

The block designs $\mathcal{D}$ and $\mathcal{H}$ are called *isomorphic* if there is a bijection of the set of points of $\mathcal{D}$ onto the set of points of $\mathcal{H}$ that induces a bijection of the blocks of $\mathcal{D}$ onto the blocks of $\mathcal{H}$. It happens that any two designs with parameters (7, 3, 1) are isomorphic, and so we speak of *the* (7, 3, 1) design.

And now, let's talk about error-correcting codes and their connections with (7, 3, 1).

| | | | |
|---|---|---|---|
| $D_1$ : | {1, 2, 4} | $H_1$ : | {1, 2, 3} |
| $D_2$ : | {2, 3, 5} | $H_2$ : | {1, 4, 5} |
| $D_3$ : | {3, 4, 6} | $H_3$ : | {1, 6, 7} |
| $D_4$ : | {4, 5, 7} | $H_4$ : | {2, 4, 6} |
| $D_5$ : | {5, 6, 1} | $H_5$ : | {2, 5, 7} |
| $D_6$ : | {6, 7, 2} | $H_6$ : | {3, 4, 7} |
| $D_7$ : | {7, 1, 3} | $H_7$ : | {3, 5, 6} |
| (*a*) | The design $\mathcal{D}$ | (*b*) | The design $\mathcal{H}$ |

**Figure 2** (7, 3, 1) as (a) differences mod 7 and as (b) three-bit strings

## Binary Hamming codes

Let's begin with two parties, Alice and Bob, who want to communicate with each other. Alice is sending a message to Bob. The message is expressed in some way as a sequence of strings of characters or *codewords*, which are sent to a receiver, one at a time. Errors can happen in the process, so the string Bob receives may fail to be a codeword. They can stop there, or they may try to correct the error. In every case we will consider, Alice will build some extra information into each codeword, and we will describe how this is done. Bob will use the extra information to test a string for an error and—if there is an error—to replace the bad string with the "closest" codeword (in the sense we'll describe). We are not concerned with the process by which the original message is translated into codewords or vice versa. For this paper, at least, we are only concerned with Alice sending one codeword at a time to Bob, possibly with some characters changed by error, and then with Bob trying to reconstruct the original codeword.

Mathematical schemes to deal with such errors first appeared in the 1940s in the work of several researchers, including Claude Shannon, Richard Hamming, and Marcel Golay. These researchers saw the need for something that would automatically detect and correct errors in signal transmissions across channels that were noisy and hence were likely to produce such errors. Their work led to a new branch of mathematics called *coding theory*—specifically, the study of error-detecting and error-correcting codes. They modeled these signals as sets of $m$-long strings called *blocks*, to be taken from a fixed alphabet of size $q$; a particular set $\mathcal{C}$ of such blocks, or *codewords*, is called a *$q$-ary code of length $m$*.

If $q$ is a prime number, then $\mathcal{C}$ is called *linear* provided the codewords of $\mathcal{C}$ form a subspace of the $m$-dimensional vector space of $(\mathbb{Z}/q\mathbb{Z})^m$, the $m$-dimensional vector space over the field of integers mod $q$. A basis for such a linear code is called a *generating set* for the code. In this paper, *all of the codes we look at are linear codes*.

To *detect* errors means to determine that a codeword was incorrectly received; to *correct* errors means to determine the right codeword in case it *was* incorrectly received. Just how this correction happens will vary from code to code.

The fact that $d$ errors in transmission change $d$ characters in a block gives rise to the idea of distance between blocks. If $v$ and $w$ are $n$-blocks, then the *(Hamming) distance* $D(v, w)$ is the number of positions in which $v$ and $w$ differ. Thus, $D(11001, 10101) = 2$ and $D(1102002, 2011012) = 5$. If Alice sends the block $v$ and Bob receives the block $w$, then $D(v, w)$ errors occurred while sending $v$. The *Hamming sphere of radius $d$* about an $n$-block $w$, denoted $S(w, d)$, is the set of all $n$-blocks whose Hamming distance from $w$ is at most $d$. Finally, the *(Hamming) weight* of a codeword is the number of nonzero characters.

It follows that if the words in a code are all "far apart" in the Hamming distance sense, then we can detect errors. Even better, if we assume that only a few errors are

received, then we can sometimes change the received block to the correct codeword. Let us now look at an example of an error-correction scheme.

A simple example of a binary code of length 3 consists of only two codewords, 000 and 111. If Bob receives 010, then it is most likely that Alice sent 000 and so the intended message was **0**; this is the *triplication* or *majority-vote* code. Effectively, a three-bit codeword consists of one "message bit" sent three times. More generally, a codeword of length $n$ contains a certain number $k$ of *message bits*, and the other $n - k$ *check bits* are used for error detection and correction. Such a code is called an $(n, k)$ code: the triplication code is a (3, 1) code.

We have presented $k$ as the number of message bits, but it can be defined more clearly as the dimension of the subspace consisting of the codewords. This makes sense only for linear codes—but in this paper, as previously mentioned, we are only concerned with linear codes.

The *minimum distance* of a code is the smallest distance between its codewords; this minimum distance determines the code's error detection and correction features. For example, a code with minimum distance five will detect up to four errors and correct up to two. You can show that a code with minimum distance $d$ will detect up to $d - 1$ errors and correct up to $\lfloor (d-1)/2 \rfloor$ errors. We see that if the Hamming spheres $S(w, d)$ of radius $d$ about all codewords $w$ are pairwise disjoint, then the code can correct up to $d$ errors. Maximum efficiency in an $(n, k)$ $d$-error correcting code $\mathcal{C}$ occurs when every string of length $n$ is either a codeword or at a distance of at most $d$ from a unique codeword—equivalently, when the Hamming spheres of radius $d$ about all codewords partition the set of all $n$-blocks. This is a rare event, and a code with this property is called *perfect*. In this paper, *all of the codes we look at are perfect codes*.

Hamming's first error-correcting scheme was a perfect one-error correcting code of length seven with four message bits, three check bits, and minimum distance 3; hence, it could correct all errors in which a single bit was received incorrectly. Golay extended Hamming's work and constructed a family of $(2^n - 1, 2^n - 1 - n)$ linear binary perfect one-error correcting codes of minimum distance 3 for all $n \geq 2$. These are now known as the binary Hamming codes, and they include both Hamming's original (7, 4) code and the (3, 1) triplication code. The notation $H(m, k)$ refers to a linear binary perfect one-error correcting code of length $m$ and dimension $k$.

$H(7, 4)$, Hamming's first code—the perfect single-error correcting code of length 7—was described in 1948 in [**17**, p. 418], as follows:

> Let a block of seven [binary] symbols be $X_1, X_2, \ldots, X_7$. Of these, $X_3$, $X_5$, $X_6$, and $X_7$ are the message symbols and chosen arbitrarily by the source. The other three are redundant and calculated as follows:
>
> $$X_4 \text{ is chosen to make } \alpha = X_4 + X_5 + X_6 + X_7 \text{ even}$$
> $$X_2 \text{ is chosen to make } \beta = X_2 + X_3 + X_6 + X_7 \text{ even}$$
> $$X_1 \text{ is chosen to make } \gamma = X_1 + X_3 + X_5 + X_7 \text{ even.}$$
>
> When a block of seven is received, $\alpha$, $\beta$ and $\gamma$ are calculated and if even, called zero, if odd, called one. The binary number $\alpha\beta\gamma$ then gives the subscript of the $X_i$ that is incorrect (if **0**, there was no error).

Now, this procedure determines $\alpha$, $\beta$ and $\gamma$ mod 2 in the following way. Suppose exactly one of the seven bits, say $X_j$, is incorrect. Since $\alpha = X_4 + X_5 + X_6 + X_7$ adds

up the $X_i$ whose high bit equals 1, it follows that $\alpha = 1$ if and only if $j = 4, 5, 6$ or 7, that is, if the high bit of $X_j$ is 1. Similarly, $\beta = X_2 + X_3 + X_6 + X_7$ adds up the $X_j$ whose middle bit equals 1, so it follows that $\beta = 1$ if and only if $j = 2, 3, 6$ or 7, i.e., if the middle bit of $X_j$ is 1. Finally, $\gamma = X_1 + X_3 + X_5 + X_7$ adds up the $X_j$ whose low bit equals 1, and so $\gamma = 1$ if and only if $j = 1, 3, 5$ or 7, i.e., if the low bit of $X_j$ is 1. Thus, $X_j$ affects those, and only those, of $\alpha$, $\beta$, and $\gamma$ whose sum contains $X_j$.

Another way to describe the decoding procedure is that if $X = (X_1, \ldots, X_7)$ is a seven-bit string, then compute $v = P \cdot X^t$, where

$$P = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

$P$ is constructed in such a way that if the vector $v$ is identical to the $i$th column of $P$, then $X_i$ is the incorrect bit, and if $v = \mathbf{0}$, then there is no error.

The free choices for the four message symbols shows that there are 16 codewords, and the condition that $P \cdot v^t = \mathbf{0}$ (when $v$ is a codeword) means that the vector $v$ is in the (right) null space of the matrix $P$. Thus, the 16 codewords are closed under both addition and scalar multiplication by 0 and 1. In short, the codewords form a four-dimensional subspace of $(\mathbb{Z}/2\mathbb{Z})^7$ and we see that the above code is a linear code. More generally, if $\mathcal{C}$ is a linear code that is the null space of a matrix $Q$, then we call $Q$ the *parity check matrix* for the code.

Hamming's scheme, then, takes every seven-long binary string with a single error and corrects that error, producing the corrected seven-bit codeword—whence the name "binary single error-correcting code of length 7." Since this code has length 7 and dimension 4, we call it the binary Hamming code $H(7, 4)$. The smallest binary Hamming code is $H(3, 1)$, the so-called triplication code: Each bit is sent three times, and the parity-check matrix is $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$.

**(7, 3, 1) and the original Hamming code.** The parity-check matrix $P$ has another interesting feature. Write $P = [P_1, \ldots, P_7]$—thus, $P_i$ is the $i$th column of $P$—and consider the set $C_i$ of columns of $P$ whose dot products with $P_i$ equal zero:

Do the $C_i$ on the left in FIGURE 3 look familiar? They should. In fact, they are a rearrangement of the blocks $H_1, \ldots, H_7$ in the right-hand column of FIGURE 2, and we have another way to produce the (7, 3, 1) design. This is also our first example of a *Singer design*, a topic we'll talk about in a later section.

| $i$ | $P_i$ | binary $C_i$ | decimal $C_i$ |
|---|---|---|---|
| 1 | 001 | {010, 100, 110} | {2, 4, 6} |
| 2 | 010 | {001, 100, 101} | {1, 4, 5} |
| 3 | 011 | {011, 100, 111} | {3, 4, 7} |
| 4 | 100 | {001, 010, 011} | {1, 2, 3} |
| 5 | 101 | {010, 101, 111} | {2, 5, 7} |
| 6 | 110 | {001, 110, 111} | {1, 6, 7} |
| 7 | 111 | {011, 101, 110} | {3, 5, 6} |

| $i$ | $B_i$ | $\{j : B_{i,j} = 1\}$ |
|---|---|---|
| 1 | 1110000 | {1, 2, 3} |
| 2 | 1001100 | {1, 4, 5} |
| 3 | 1000011 | {1, 6, 7} |
| 4 | 0101010 | {2, 4, 6} |
| 5 | 0100101 | {2, 5, 7} |
| 6 | 0011001 | {3, 4, 7} |
| 7 | 0010110 | {3, 5, 6} |

**Figure 3** The Singer (7, 3, 1) design (left) and the seven codewords of weight 3 (right)

**(7, 3, 1), Hamming, and the three-circle Venn diagram.** A second appearance of (7, 3, 1) in this code is in the table on the right side of FIGURE 3. This table comes from the seven codewords of weight 3. The blocks $B_i = B_{i,1} \dots B_{i,7}$ are the codewords, the points $j$ are the integers $1, \dots, 7$, and $j \in B_i$ if and only if $B_{i,j} = 1$—another (7, 3, 1) design.

Finally, Hamming's system of three congruences (mod 2) has a nice pictorial interpretation, as follows. Draw the usual three-circle Venn diagram for three sets. Next, associate the region that is in all three sets with $X_7$, associate the regions that are in exactly two of the sets with $X_3$, $X_5$, and $X_6$, and associate the regions that are in exactly one of the sets with $X_1$, $X_2$, and $X_4$. We see that each region of the diagram is associated with exactly one of the $X_i$, and each $X_i$ appears exactly once.

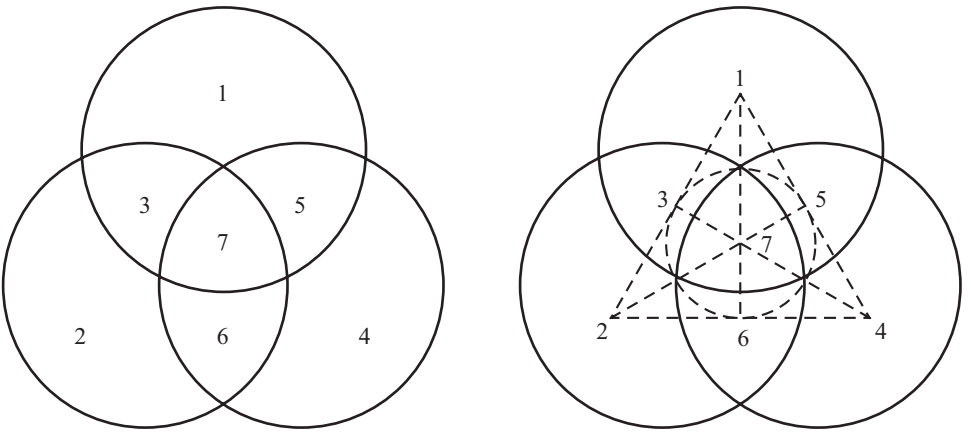


**Figure 4** The three-circle Venn diagram (left) with another instance of (7, 3, 1) (right)

Hamming's scheme can be realized by placing $X_i$ in its corresponding region, then the number of 1s in each of the circles must be even. Pictorially, if exactly one $X_i$ is switched from $x$ to $1 - x$, then it will be the value in the region contained in exactly those circles with an odd number of 1s. As a bonus, this picture also shows us one more appearance of (7, 3, 1) (on the right-hand side of FIGURE 4), and so the Hamming (7, 4) code gives us three different views of (7, 3, 1)!

The earliest Hamming codes were designed to correct errors in messages encoded as bit strings, and the underlying arithmetic was done in the two-element field. In the next section, we extend the results of this section to correct errors in messages where the arithmetic is performed in a finite field $\mathbb{F}_q$, where $q$ is an odd prime.

## *q*-ary Hamming codes

Let $q$ be a prime. A *$q$-ary code of length $m$* is a collection of strings of length $m$ over an alphabet of $q$ elements. Since $q$ is a prime, we may take these elements to be the finite field $\mathbb{F}_q = \{0, 1, \dots, q-1\}$. As we have seen, if a code can correct up to $d$ errors in messages of length $n$, then every string of length $n$ is at a Hamming distance at most $d$ from a codeword and so is contained within a sphere $S(w, d)$ of Hamming radius $d$ about some codeword $w$.

We now show how to construct $q$-ary Hamming codes—that is, $q$-ary perfect one-error correcting codes—so we consider the Hamming spheres of radius 1. If $w$ is a codeword of length $n$, then there are $n$ positions where a single error can occur, and

for each position, there are $(q-1)$ possible errors. Thus, for $q$-ary codes, the sphere $S(w,1)$ contains the codeword $w$ together with all $n(q-1)$ strings with exactly one error. It follows that if a $q$-ary code $\mathcal{C}$ corrects all single errors, then the spheres of radius 1 about every codeword in $\mathcal{C}$ are pairwise disjoint. Hence, the set of all $q^n$ $q$-ary strings of length $n$ contains the union of these spheres. If such a code $\mathcal{C}$ is perfect, then every such string belongs to one of these spheres. Hence, if $\mathcal{C}$ is perfect and contains $W$ codewords, then we see that

$$W = \frac{q^n}{1+n(q-1)}.$$

The right-hand side is called the *Hamming* or *sphere-packing* bound, and a single-error correcting code is perfect exactly when the Hamming bound is attained.

For a Hamming code of length $n$, we see that $W(1+n(q-1)) = q^n$; since $q$ is a prime, this means that $1+n(q-1)$ must be a power of $q$. Thus, $1+n(q-1) = q^k$ for some positive integer $k$; we solve this for $n$ and see that $n = \frac{q^k-1}{q-1}$, and so the code contains $q^{n-k}$ codewords. It follows that we may encode all $q$-ary messages of length $n-k$ in a way that corrects each error pattern involving a single incorrect character. In short, a codeword contains $n-k$ message digits and $k$ so-called parity-check digits.

Thus, if a perfect $q$-ary Hamming code exists, then its length is necessarily equal to $n = \frac{q^k-1}{q-1}$ for some $k$. Now, we know that "necessary" does not mean "sufficient." But in fact, $q$-ary Hamming codes of length $n$ having $n-k$ message digits do exist for all $n$ and $k$, and we now show how to construct such $\left(\frac{q^k-1}{q-1}, \frac{q^k-1}{q-1}-k\right)$ codes. These are linear codes, as they are realized as $n-k$-dimensional subspaces of an $n$-dimensional vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$.

Let $Q$ be a $k \times m$ matrix over $\mathbb{F}_q$ such that for fixed $k$, (1) no two columns of $Q$ are linearly dependent, and (2) for the given $k$, $m$ is as large as possible. Condition (1) states that no two columns of $Q$ are multiples of each other. Now, each nonzero column vector $v$ has $q-1$ nonzero scalar multiples, so (1) implies that we may choose at most one of these. We collect one vector from each set of $q-1$ nonzero multiples of a given vector until we cannot proceed further. Since there are $q^k-1$ nonzero vectors of length $k$ and since these are partitioned into sets of $q-1$ nonzero multiples of a single vector, this means that we will have at least $(q^k-1)/(q-1)$ columns. But every nonzero vector is a multiple of exactly one of the vectors we have chosen, so the desired maximum number $m$ of columns is equal to $(q^k-1)/(q-1)$. Sounds familiar, doesn't it? Indeed it is. The value of $m$ we seek is precisely the number $n$ from the preceding several paragraphs.

To encode a message string, we mimic what is done for the binary Hamming codes, with slight variations. Let $q$, $n$ and $k$ be as above, and let $Q$ be a $k \times n$ matrix constructed as follows. Let the first $k$ columns of the parity-check matrix be the identity matrix $I_k$ of order $k$; these $k$ positions will determine the parity digits. The other $n-k$ columns represent the message digits: Placed in increasing numerical order, they are the base-$q$ representations of the non-powers of $q$ between 1 and $q^k-1$ whose most significant digit is a 1. One can check that $Q$ has the properties (1) and (2) mentioned in the previous paragraph.

For the Hamming $q$-ary code of dimension $n-k$, the parity-check matrix will have $k$ rows and $n$ columns. That is, a $q$-ary string of length $n$ contains $n-k$ message digits and $k$ parity digits. In all, the parity-check matrix has $(q^k-1)/(q-1)$ columns. Thus, a ternary Hamming code of length $(3^4-1)/(3-1) = 40$ will have four parity positions and 36 message positions. A base-5 Hamming code of length $(5^3-1)/(5-1) = 31$ has five parity positions and 26 message positions.

Let's illustrate this with the ternary Hamming code of length $13 = (3^3 - 1)/(3 - 1)$. The parity-check matrix $T$ for this code is given by

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 0 & 1 & 1 & 2 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$$

To encode the message $(m_4, m_5, m_6, m_7, m_8, m_9, m_{10}, m_{11}, m_{12}, m_{13})$, determine the values of $c_1$, $c_2$ and $c_3$ so as to make the vector $(c_1, c_2, c_3, m_4, m_5, m_6, m_7, m_8, m_9, m_{10}, m_{11}, m_{12}, m_{13})$ an element of the right null space of $T$. That is, pick $c_1$, $c_2$ and $c_3$ to satisfy the congruences

$$c_1 + m_6 + m_7 + m_8 + m_9 + m_{10} + m_{11} + m_{12} + m_{13} \equiv 0 \pmod 3,$$

$$c_2 + m_4 + m_5 + m_8 + m_9 + m_{10} + 2m_{11} + 2m_{12} + 2m_{13} \equiv 0 \pmod 3, \text{ and}$$

$$c_3 + m_4 + 2m_5 + m_6 + 2m_7 + m_9 + 2m_{10} + m_{12} + 2m_{13} \equiv 0 \pmod 3.$$

For example, applying this procedure to the message (1, 1, 2, 1, 0, 0, 1, 2, 1, 1) yields $c_1 = 1$, $c_2 = 2$, and $c_3 = 0$, and so the associated codeword is (1, 2, 0, 1, 1, 2, 1, 0, 0, 1, 2, 1, 1).

More generally, let $v^t$ denote the transpose of $v$. For a message $(x_{k+1}, \ldots, x_n)$ of length $n - k = \frac{q^k - 1}{q-1} - k$, we determine $k$ check digits $c_1, \ldots, c_k$ such that $T \cdot (c_1, \ldots, c_k, x_{k+1}, \ldots, x_n)^t$ is the zero vector of length $n$.

To decode a message $v$, calculate $w = T \cdot v^t$. If $w = \mathbf{0}$, then $v$ is a codeword. If not, then for some nonzero integer $a$ mod $q$ and some positive integer $j$, $w = aT_j$. To correct the error, subtract $a$ (mod $q$) from the $j$th component of $P_j$.

To see how this works, let's look at an example with the ternary Hamming code of length 13. Suppose we receive the string $z = (2, 2, 0, 0, 0, 1, 0, 0, 2, 1, 1, 2, 0)$. We compute $w = T \cdot z^t = (0, 2, 1)$ mod 3; this is nonzero, so there was an error in transmission. Assuming that there was an error in only one character, we see that $w = (0, 1, 2) \equiv 2T_5$ mod 3. In the above decoding scheme, this means that $a = 2$, so we subtract 2 (mod 3) from the fifth component of $z$. The result is the vector

$$v = (2, 2, 0, 0, 0 - 2, 1, 0, 0, 2, 1, 1, 2, 0) \equiv (2, 2, 0, 0, 1, 1, 0, 0, 2, 1, 1, 2, 0) \bmod 3.$$

Sure enough, $T \cdot v^t \equiv (0, 0, 0)$ mod 3—as claimed.

Finally, we need to show that the above code has minimum distance three. As in the binary case, ours is a linear code, so the minimum distance between codewords is equal to the minimum weight of a nonzero codeword. Let's prove this now.

Note that the parity-check matrix $T$ of our Hamming $q$-ary code of dimension $n - k$ has $k$ rows and $n$ columns. By construction, the columns of $T$ are nonzero and pairwise linearly independent. Thus, there are no codewords of weights 1 or 2, so the minimum weight of a nonzero codeword is at least 3. But columns $T_{k-1}$, $T_k$ and $T_{k+1}$ are linearly dependent because $T_{k-1} + T_k - T_{k+1} = \mathbf{0}$. Hence, the $n - k$-long vector $v$ with $v_{k-1} = v_k = 1$ and $v_{k+1} = -1$ and zeros everywhere else is a codeword of weight 3—as claimed.

Now, you might wonder about the usefulness of $q$-ary codes for $q \geq 3$. Wonder no more: Ternary error-correcting codes have made their way into the world of card magic. Chapter Q (for Queen) of Colm Mulcahy's recent book [**8**]—a great read, by the way—includes a variety of card tricks that use the ternary (4, 2) Hamming code with parity-check matrix

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix}.$$

Does this matrix $T$ have a block-design connection, similar to that enjoyed by Hamming's parity-check matrix $T$? Indeed it does. If $T_i$ the $i$th column of $T$ and $D_i$ is the set of columns of $T$ whose dot products with $D_i$ equal zero, here's what we get:

| $i$ | $T_i$ | ternary $D_i$ | columns $j$ for $T_j \in D_i$ |
|---|---|---|---|
| 1 | 100 | {010, 001, 011, 012} | {2, 3, 4, 5} |
| 2 | 010 | {100, 001, 101, 102} | {1, 3, 6, 7} |
| 3 | 001 | {100, 010, 110, 120} | {1, 2, 8, 11} |
| 4 | 011 | {100, 012, 112, 121} | {1, 5, 10, 12} |
| 5 | 012 | {100, 011, 111, 122} | {1, 4, 9, 13} |
| 6 | 101 | {010, 102, 112, 122} | {2, 7, 10, 13} |
| 7 | 102 | {010, 101, 111, 121} | {2, 6, 9, 12} |
| 8 | 110 | {001, 120, 121, 122} | {3, 11, 12, 13} |
| 9 | 111 | {012, 102, 111, 120} | {5, 7, 9, 11} |
| 10 | 112 | {011, 101, 112, 120} | {4, 6, 10, 11} |
| 11 | 120 | {001, 110, 111, 112} | {3, 8, 9, 10} |
| 12 | 121 | {011, 102, 110, 121} | {4, 7, 8, 12} |
| 13 | 122 | {012, 101, 110, 122} | {5, 6, 8, 13} |

**Figure 5** The Singer (13, 4, 1) design

You can verify that in FIGURE 5, the $D_i$ are the blocks of a (13, 4, 1) design on the columns of $T$, and this is no accident. In the next section, we explore this connection between parity-check matrices for $q$-ary Hamming codes and certain block designs. These block designs arise in the context of finite projective geometries over $\mathbb{F}_q$, and R. C. Bose describes them in his 1939 landmark paper on combinatorial designs [**3**]. Let's look at these designs now.

## Singer designs

Let $n$ be a positive integer, and let $U_n = \{(x_0, x_1, \ldots, x_n) : x_i \in \mathbb{F}_q\} - \{(0, \ldots, 0)\}$ be the set of all nonzero $(n+1)$-tuples with elements in the field $\mathbb{F}_q$. Define an equivalence relation $\sim$ on $U_n$ by $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ provided there exists a nonzero constant $\lambda$ such that $x_i = \lambda y_i$ for all $i$. We define the $n$-dimensional projective space $PG(n, q)$ over $\mathbb{F}_q$ to be the set of all $\sim$-equivalence classes in $U_n$.

A point of $PG(n, q)$ is an equivalence class of $(n+1)$-tuples. For an example, consider the space $PG(3, 5)$ of dimension 3 over the five-element field. The nonzero scalar multiples of $p = (1, 4, 3, 3)$ are $p$ itself, $2p = (2, 3, 1, 1)$, $3p = (3, 2, 4, 4)$, and $4p = (4, 1, 2, 2)$, and so in $PG(3, 5)$, $p$ represents the class of its nonzero multiples. (The same letter refers to both the element and its equivalence class—the key is to remember that scalar multiples represent the same class.) The lattice of subspaces of $PG(n, q)$ corresponds to the lattice of subspaces of $\mathbb{F}_q^{n+1}$.

There are $q^{n+1} - 1$ nonzero vectors in $\mathbb{F}_q^{n+1}$, and each nonzero vector is in a $\sim$-equivalence class containing $q - 1$ scalar multiples. Hence, $PG(n, q)$ contains $(q^{n+1} - 1)/(q - 1)$ elements, which are the points.

In [**3**], R. C. Bose proved the following theorem about an interesting class of block designs, now known as *Singer designs* after their discoverer James Singer, who first described them in [**18**].

**Bose's Theorem.** *The points and $(n-1)$-dimensional subspaces of $PG(n,q)$ are the points and blocks, respectively, of a*

$$\left(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}\right)$$

*symmetric balanced incomplete block design.*

To see why this is so, we first review some linear algebra. Let $H$ be a $d$-dimensional subspace of an $n$-dimensional vector space. The *(right) null space* $H^\perp$ of $H$ is the set of vectors $v$ for which $Hv = \mathbf{0}$—left null spaces are defined analogously—and the *nullity* of $H$ is the dimension of $H^\perp$. The rank-nullity theorem tells us that the dimension of $H^\perp$ is equal to $n-d$. Thus, if $B$ is an $n$-dimensional subspace of $\mathbb{F}_q^{n+1}$, then by the rank-nullity theorem, $B^\perp$ has dimension 1.

Now, let $K$ be a $d$-dimensional subspace of $PG(n,q)$. Then $K$ corresponds to a $d+1$-dimensional subspace of $\mathbb{F}_q^{n+1}$, so its null space has dimension $n+1-(d+1) = n-d$. Projectively, this null space corresponds to an $n-d-1$-dimensional subspace of $PG(n,q)$. In particular, if $K$ is an $(n-1)$-dimensional subspace of $PG(n,q)$, then its null space has dimension $n-(n-1)-1 = 0$. In short, the null space of an $(n-1)$-dimensional subspace of $PG(n,q)$ is a point, and it follows that distinct $(n-1)$-dimensional subspaces have distinct null spaces. Hence, the points and the $(n-1)$-dimensional subspaces—let's call the latter *blocks*—are in one-to-one correspondence, and there are $v = (q^{n+1}-1)/(q-1)$ of each.

Let $B$ be the block whose null space is the point $(a_0, \ldots, a_n)$. Then every element $w = (x_0, \ldots, x_n) \in B$ satisfies $\sum_{i=0}^{n} a_i x_i = 0$; without loss of generality, suppose $a_0 \neq 0$. Then each of the $q^n - 1$ nonzero choices of $x_1, \ldots, x_n$ determines a unique value of $x_0$. However, since the $q-1$ scalar multiples of a solution vector $w$ are considered the same, we divide out by that quantity and see that a block contains $k = (q^n-1)/(q-1)$ points. A similar argument shows that every point is contained in $k$ blocks.

Finally, two blocks are either equal or intersect in an $(n-2)$-dimensional subspace of $PG(n,q)$, and repeating the above argument shows that the intersection of distinct blocks has $\lambda = (q^{n-1}-1)/(q-1)$ points, and each pair of distinct points belongs to $\lambda$ blocks.

In short, the collection of subspaces of dimension $n-1$ in $PG(n,q)$ forms a symmetric $(v,k,\lambda)$ block design whose elements are the points of $PG(n,q)$, and this completes the proof of Bose's theorem. These are called Singer designs, for reasons that will be made clear in the next section.

We now make a connection between Hamming codes and Singer designs, and the connection is this.

**Theorem (The Hamming–Singer Connection).** *Let $q$ be a prime and let $n$ be a positive integer, and let $P$ be the parity-check matrix for the $q$-ary Hamming code with $n+1$ parity-check digits. Then*

- *The null spaces of the columns of $P$ form a symmetric block design with the columns as points and the null spaces as blocks.*
- *This design contains $v = (q^{n+1}-1)/(q-1)$ points and the same number of blocks.*
- *Each block contains $k = (q^n-1)/(q-1)$ points, and each point is in the same number of blocks.*

- *Each pair of points belongs to* $\lambda = (q^{n-1} - 1)/(q - 1)$ *blocks together. In other words:*
- *The columns of a parity-check matrix of a Hamming*

$$\left(\frac{q^{n+1} - 1}{q - 1}, \frac{q^{n+1} - 1}{q - 1} - (n + 1)\right)$$

*code are the points of a* $(v, k, \lambda)$ *Singer design with* $v, k,$ *and* $\lambda$ *as above.*

The fact that the columns of $P$ are pairwise linearly independent guarantees that those columns can be viewed as the points of $PG(n, q)$; the Hamming–Singer connection then follows from previous reasoning. In particular, we see that for $n = q = 2$, we have $v = 7, k = 3$ and $\lambda = 1$, and so the Singer (7, 3, 1) design is another name for (7, 3, 1). See FIGURE 3).

## Singer difference sets in *PG*(*n, q*)

James Singer (1906–1976) graduated from Cornell in 1926 and received a Ph.D. from Princeton in 1931 with a dissertation in topology directed by the eminent topologist J. W. Alexander. He was on the mathematics faculty of Brooklyn College from 1936 to 1974 and by all accounts was an influential and beloved teacher. He became interested in finite projective geometry, and in his 1938 paper [**18**], Singer proved the following theorem.

**Singer's Theorem.** *Let* $D$ *be an* $(n - 1)$*-dimensional subspace of* $PG(n, q)$*. Then there is a bijective transformation carrying the* $v = (q^{n+1} - 1)/(q - 1)$ *points of* $PG(n, q)$ *onto the integers* $\{0, 1, \ldots, v - 1\}$ *in such a way that the resulting integers corresponding to the* $k = (q^n - 1)/(q - 1)$ *points of* $D$ *have the following property. Namely, every nonzero integer mod* $v$ *can be expresses as the difference between distinct elements of* $D$ *in exactly* $\lambda = (q^{n-1} - 1)/(q - 1)$ *ways.*

In short, Singer proved that with $v, k$ and $\lambda$ as above, each block of a Singer $(v, k, \lambda)$ design is what he called a *difference set*. More generally, if $v, k$ and $\lambda$ are positive integers, then a $(v, k, \lambda)$ *difference set* is a $k$-element subset $D = \{d_1, \ldots, d_k\}$ of $\{1, 2, \ldots, v\}$ such that every nonzero integer (mod $v$) can be expressed as a difference $d_i - d_j$ of the elements of $D$ in exactly $\lambda$ ways. Later, researchers expanded the definition to arbitrary finite groups, in which a $(v, k, \lambda)$ difference set in a $v$-element group $G$ is a $k$-element subset $D$ of $G$ such that every nonidentity element of $G$ can be expressed in exactly $\lambda$ ways as a product $ab^{-1}$ of elements of $D$.

We began the 2002 paper [**4**] by showing that the subset $Q_7 = \{1, 2, 4\}$ of $\mathbb{Z}$ mod 7 is a (7, 3, 1) difference set. For, in $\mathbb{Z}$ mod 7, $1 = 2 - 1, 2 = 4 - 2, 3 = 4 - 1, 4 = 1 - 4, 5 = 2 - 4,$ and $6 = 1 - 2$. Thus, $Q_7$ is a (7, 3, 1) difference set. We then showed that (a) if $p = 4n + 3$ is a prime, then the set $Q_p$ of nonzero squares mod $p$ is a $(4n + 3, 2n + 1, n + 1)$ difference set and (b) if $D$ is a $(v, k, \lambda)$ difference set, then the $v$ translates $D + i = \{x + i \bmod v \mid x \in D\}$ form a symmetric $(v, k, \lambda)$ block design. In particular, the seven translates of $Q_7$ mod 7 are the blocks $D_1, \ldots, D_7$ in the left-hand column of FIGURE 2. Similarly, each of the nonzero integers mod 11 can be represented in exactly two ways as a difference of distinct elements of $Q_{11} = \{1, 3, 4, 5, 9\}$, and the 11 translates $Q_{11} + i$ mod 11 form a symmetric (11, 5, 2) block design.

A symmetric design on $V = \{0, \ldots, v - 1\}$ is called *cyclic* if the $v$ blocks are the $v$ translates $D + i$ mod $v$ of some fixed block $D$. Singer's next theorem tells us in such a design, every block is a difference set.

**Theorem.** *Let $\mathcal{B} = \{B_0, B_1, \ldots, B_{v-1}\}$ be the blocks of a cyclic $(v, k, \lambda)$ design on the set of points $V = \{0, 1, \ldots, v-1\}$, Then each block $B_i$ is a $(v, k, \lambda)$ difference set.*

Let's prove this.

To simplify the proof, we assume that $0 \in B_0$. Thus, $B_0 = \{x_1, \ldots, x_{k-1}, 0\}$ for some $x_i \in V$, $1 \leq k-1$, $x_i \neq 0$. We show that $B_0$ is a $(v, k, \lambda)$ difference set. Since the design is symmetric, each point is in $k$ blocks and there are $v$ blocks in all. Since the design is cyclic, we see that $B_j = \{x_1 + j, \ldots, x_{k-1} + j, j\}$ for $0 \leq j \leq v-1$.

Now, let $d$ be any nonzero element of $V$. Then $d$ and 0 are in exactly $\lambda$ blocks together—that is, for $\lambda$ values of $j$, $d, 0 \in B_j$. A block has no repeated elements, so if $d, 0 \in B_j$, then $d = x_r + j$ and $0 = x_s + j$ for distinct $x_r, x_s \in B_0$. Thus, $d = d - 0 = x_r - x_s$ for exactly $\lambda$ pairs $(x_r, x_s)$ of distinct elements of $B_0$. Since $d$ was arbitrary, it follows that every nonzero number mod $v$ can be expressed as a difference of elements of $B_0$ in exactly $\lambda$ ways. In short, $B_0$ is a $(v, k, \lambda)$ difference set.

Thus, if $a, b \in B_j$, then $a = x_r + j$, $b = x_s + j$ for $x_r, x_s \in B_0$, and so $a - b = x_r + j - (x_s - j) = x_r - x_s$. Hence, the differences of elements in $B_j$ are the same as the differences of elements in $B_0$, and so each block $B_j$ is a $(v, k, \lambda)$ difference set—as claimed.

More generalization is possible. In fact, there is a way to make the Singer block designs contained in $PG(n, q)$ into cyclic designs. Proving this is tedious, so we will not pursue it. For a proof, see [**20**, pp. 79–82].

We now explore a fascinating connection (7, 3, 1) has with a number system that superficially resembles the complex numbers and to which mathematicians were led by asking questions about sums of squares.

## Sums of squares, the octonions, and the sedenions

Squares and their sums have fascinated the mathematical world for millennia, beginning with the Pythagorean theorem. Euclid gives a proof of the Pythagorean theorem in Book I, Proposition 47 of The Elements. Book X, Proposition 29, Lemma 1 gives a general formula for triples $(x, y, z)$ of integers such that $x^2 + y^2 = z^2$. In modern notation, if $a$ and $b$ are relatively prime integers of opposite parity, set $x = a^2 - b^2$, $y = 2ab$, and $z = a^2 + b^2$; then $x^2 + y^2 = z^2$.

Several hundred years later, Diophantus (*ca.* 250 CE) made an observation in the solution to Problem III.22 of his *Arithmetica*, an observation that implicitly contains the identity

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2,$$

which gives the product of two sums of two squares as a sum of two squares. Diophantus does not supply a proof, but almost a millennium later, Leonardo of Pisa (1175–1240) includes this two-squares identity—with proof—in his *Liber quadratorum* (The Book of Squares).

In 1748, Euler proved the four square identity, namely that the product of two sums of four squares is again a sum of four squares, showing that if $a_1, \ldots, a_4$ and $b_1, \ldots, b_4$ are numbers, then

$$\begin{aligned}(a_1^2 + a_2^2 + a_3^2 + a_4^2)&(b_1^2 + b_2^2 + b_3^2 + b_4^2)\\ &= (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2\\ &\quad + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2.\end{aligned}$$

Lagrange used this identity in his 1770 proof that every positive integer can be written as a sum of four squares of integers. The identities of Diophantus and Euler raised the question, "Are there other identities like this?"

One such identity for sums of eight squares was first found by the Danish mathematician Ferdinand Degen in 1818 . The eight-squares identity states that if $a_0, \ldots, a_7$ and $b_0, \ldots, b_7$ are numbers, then

$$\begin{aligned}
&(a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2) \\
&\quad \times (b_0^2 + b_1^2 + b_2^2 + b_3^2 + b_4^2 + b_5^2 + b_6^2 + b_7^2) \\
&\quad = (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7)^2 \\
&\qquad + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2 + a_4b_5 - a_5b_4 - a_6b_7 + a_7b_6)^2 \\
&\qquad + (a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1 + a_4b_6 + a_5b_7 - a_6b_4 - a_7b_5)^2 \\
&\qquad + (a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0 + a_4b_7 - a_5b_6 + a_6b_5 - a_7b_4)^2 \\
&\qquad + (a_0b_4 - a_1b_5 - a_2b_6 - a_3b_7 + a_4b_0 + a_5b_1 + a_6b_2 + a_7b_3)^2 \\
&\qquad + (a_0b_5 + a_1b_4 - a_2b_7 + a_3b_6 - a_4b_1 + a_5b_0 - a_6b_3 + a_7b_2)^2 \\
&\qquad + (a_0b_6 + a_1b_7 + a_2b_4 - a_3b_5 - a_4b_2 + a_5b_3 + a_6b_0 - a_7b_1)^2 \\
&\qquad + (a_0b_7 - a_1b_6 - a_2b_5 + a_3b_4 - a_4b_3 - a_5b_2 + a_6b_1 + a_7b_0)^2.
\end{aligned}$$

At this point, mathematicians were quite hopeful that other, perhaps infinitely many, sums-of-squares identities exist. Let's rephrase the question "Are there other identities like this?" as follows. For which positive integers $n$ does there exist an identity of the form

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2, \quad \text{where } z_k = \sum_{i,j=1}^{n} A_{ijk} x_i y_j,$$

and the $A_{ijk}$ are constants independent of the values of the $x_i$ and the $y_j$?

The question was answered in 1898 by Adolph Hurwitz, who proved that such an identity exists for $n = 1, 2, 4, 8$—and for no other positive integers. He showed that each sums-of-squares identity led to an $n$-dimensional *normed algebra*. Now a normed algebra $\mathbb{A}$ is an $n$-dimensional vector space over the real numbers $\mathbb{R}$ that has two special features, namely (1) a vector multiplication that distributes over vector addition, and (2) a mapping $N : \mathbb{A} \to \mathbb{R}$ such that $N(uv) = N(u)N(v)$ for all $u, v \in \mathbb{A}$. These algebras are the real numbers $\mathbb{R}$ ($n = 1$), the complex numbers $\mathbb{C}$ ($n = 2$), Hamilton's *quaternions* $\mathbb{H}$ ($n = 4$), and the *octonions* $\mathbb{O}$ ($n = 8$). The latter is a beautiful algebraic system with a multiplication table that reveals itself as another aspect of (7, 3, 1). We will explore the octonions below, and then we will construct the analogous 16-dimensional algebra known as the *sedenions* and see just why it is not a normed algebra.

One square is easy: Because multiplication of real numbers is commutative and associative, we see that $a^2b^2 = (ab)^2$ for all real numbers $a$ and $b$. As for two squares, Diophantus (*ca.* 250 CE) had an answer. Problem III.22 of his *Arithmetica* implicitly contains the identity

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2,$$

which gives the product of two sums of two squares as a sum of two squares. As mentioned above, the normed algebras associated with the one-square and two-square identities will turn out to be the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$, respectively.

In fact, multiplication of complex numbers reflects the two-squares identity as follows. Let $z = a + bi$ and define $N(z) = a^2 + b^2$; if $w = c + di$, then $N(w) = c^2 + d^2$, and we see that $zw = ac - bd + (ad + bc)i$. Finally, we see that

$$N(zw) = (ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2) = N(z)N(w),$$

by the two-squares identity.

As for the associated normed algebra associated with the four-squares identity, that is one of the great stories in mathematics, and it came about in the following way.

During the early 1840s, William R. Hamilton was searching for a way to multiply ordered triples of real numbers, analogous to multiplication of complex numbers viewed as ordered pairs. He searched a long time and failed to find such a multiplication, but working through these unsuccessful attempts led him to one of the famous "aha!" moments in the history of mathematics. On the morning of October 16, 1843, that moment came to Hamilton while he was taking a walk. He realized in a flash of insight that the solution he sought was a multiplication of quadruples, not triples, and then, as he described in an 1865 letter to his son Archibald [**13**], "Nor could I resist the impulse—unphilosophical as it may have been—to cut with a knife on a stone of Brougham Bridge, as we passed it, the fundamental formula with the symbols, $i$, $j$, $k$; namely,

$$i^2 = j^2 = k^2 = ijk = -1,$$

which contains the Solution of the Problem, but of course, as an inscription, has long since mouldered away."

Hamilton gave the name *quaternions* to the resulting algebra $\mathbb{H}$ generated by $1$, $i$, $j$ and $k$; the multiplication table for the units $1$, $i$, $j$ and $k$ is as follows:

| $*$ | **1** | **i** | **j** | **k** |
|---|---|---|---|---|
| **1** | 1 | $i$ | $j$ | $k$ |
| **i** | $i$ | $-1$ | $k$ | $-j$ |
| **j** | $j$ | $-k$ | $-1$ | $i$ |
| **k** | $k$ | $j$ | $-i$ | $-1$ |

A quaternion is an expression of the form $x_1 + x_2i + x_3j + x_4k$, where the $x_n$ are real numbers. It is easy to see how to add these expressions term-by-term, and Hamilton's new multiplication table shows us how to multiply them. One multiplies two quaternions by using the distributive law, Hamilton's table, and the fact that $xi = ix$, $xj = jx$, and $xk = kx$ for all real numbers $x$. Hamilton showed that this multiplication is associative; however, the table shows that $ij = k = -ji$ and so multiplication is not commutative. We can define a norm on $\mathbb{H}$ by $N(x_1 + x_2i + x_3j + x_4k) = x_1^2 + x_2^2 + x_3^2 + x_4^2$, and because of the four-square identity, it follows that $N(x)N(y) = N(xy)$ for all $x, y \in \mathbb{H}$. Therefore, $\mathbb{H}$ is a four-dimensional normed algebra—that is, $\mathbb{R}^4$ equipped with a multiplication—and because of that, we can show that $\mathbb{H}$ is a *division ring*, which means that every nonzero element of $\mathbb{H}$ has a multiplicative inverse. Here's how.

We first define the *conjugate* $\overline{x}$ of a quaternion $x$ by $\overline{x_1 + x_2i + x_3j + x_4k} = x_1 - x_2i - x_3j - x_4k$. Another routine calculation shows that

$$x\overline{x} = (x_1 + x_2i + x_3j + x_4k)(x_1 - x_2i - x_3j - x_4k) = x_1^2 + x_2^2 + x_3^2 + x_4^2 = N(x).$$

Now, if $x \neq 0$, then $N(x)$ is a positive real number, and it follows that

$$x \cdot \frac{\overline{x}}{N(x)} = \frac{N(x)}{N(x)} = 1.$$

Hence, $x$ has a multiplicative inverse, and so $\mathbb{H}$ is a division algebra. Since, at that time, the only known division rings were fields, $\mathbb{H}$ was the first example of a noncommutative division ring. This unique status of $\mathbb{H}$ would last only a couple of months.

What happened next was that, the very next day, Hamilton mailed the good news about the quaternions to his friend and fellow mathematician John T. Graves. Two months later, Graves sent him a letter in which he described a multiplication on $\mathbb{R}^8$; we now call this algebra the *octonions* $\mathbb{O}$. Hamilton's quaternion multiplication uses three units $\{i, j, k\}$, each of whose squares is equal to $-1$. Graves' multiplication on $\mathbb{O}$ uses seven units $\{o_1, \ldots, o_7\}$ whose products come from the following multiplication table:

| $*$ | $\mathbf{1}$ | $\mathbf{o_1}$ | $\mathbf{o_2}$ | $\mathbf{o_3}$ | $\mathbf{o_4}$ | $\mathbf{o_5}$ | $\mathbf{o_6}$ | $\mathbf{o_7}$ |
|---|---|---|---|---|---|---|---|---|
| $\mathbf{1}$ | $1$ | $o_1$ | $o_2$ | $o_3$ | $o_4$ | $o_5$ | $o_6$ | $o_7$ |
| $\mathbf{o_1}$ | $o_1$ | $-1$ | $o_4$ | $o_7$ | $-o_2$ | $o_6$ | $-o_5$ | $-o_3$ |
| $\mathbf{o_2}$ | $o_2$ | $-o_4$ | $-1$ | $o_5$ | $o_1$ | $-o_3$ | $o_7$ | $-o_6$ |
| $\mathbf{o_3}$ | $o_3$ | $-o_7$ | $-o_5$ | $-1$ | $o_6$ | $o_2$ | $-o_4$ | $o_1$ |
| $\mathbf{o_4}$ | $o_4$ | $o_2$ | $-o_1$ | $-o_6$ | $-1$ | $o_7$ | $o_3$ | $-o_5$ |
| $\mathbf{o_5}$ | $o_5$ | $-o_6$ | $o_3$ | $-o_2$ | $-o_7$ | $-1$ | $o_1$ | $o_4$ |
| $\mathbf{o_6}$ | $o_6$ | $o_5$ | $-o_7$ | $o_4$ | $-o_3$ | $-o_1$ | $-1$ | $o_2$ |
| $\mathbf{o_7}$ | $o_7$ | $o_3$ | $o_6$ | $-o_1$ | $o_5$ | $-o_4$ | $-o_2$ | $-1$ |

Better yet, this multiplication came equipped with a norm, namely

$$N(a_0 + a_1 o_1 + \cdots + a_7 o_7) = a_0^2 + a_1^2 + \cdots + a_7^2.$$

This norm satisfies $N(ab) = N(a)N(b)$ because of Graves' other bit of news, namely his rediscovery of the eight-squares identity,

$$\begin{aligned}
&(a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2) \\
&\quad \times (b_0^2 + b_1^2 + b_2^2 + b_3^2 + b_4^2 + b_5^2 + b_6^2 + b_7^2) \\
&\quad = (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7)^2 \\
&\qquad + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2 + a_4b_5 - a_5b_4 - a_6b_7 + a_7b_6)^2 \\
&\qquad + (a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1 + a_4b_6 + a_5b_7 - a_6b_4 - a_7b_5)^2 \\
&\qquad + (a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0 + a_4b_7 - a_5b_6 + a_6b_5 - a_7b_4)^2 \\
&\qquad + (a_0b_4 - a_1b_5 - a_2b_6 - a_3b_7 + a_4b_0 + a_5b_1 + a_6b_2 + a_7b_3)^2 \\
&\qquad + (a_0b_5 + a_1b_4 - a_2b_7 + a_3b_6 - a_4b_1 + a_5b_0 - a_6b_3 + a_7b_2)^2 \\
&\qquad + (a_0b_6 + a_1b_7 + a_2b_4 - a_3b_5 - a_4b_2 + a_5b_3 + a_6b_0 - a_7b_1)^2 \\
&\qquad + (a_0b_7 - a_1b_6 - a_2b_5 + a_3b_4 - a_4b_3 - a_5b_2 + a_6b_1 + a_7b_0)^2.
\end{aligned}$$

As we have seen, the eight-squares identity was first found by the Danish mathematician Ferdinand Degen in 1818, but there is no evidence that Degen constructed the

associated multiplication on $\mathbb{R}^8$. Arthur Cayley independently rediscovered that identity when he constructed the eight-dimensional normed algebra $\mathbb{O}$ in 1845, and both he and Graves used the same method to produce their versions of $\mathbb{O}$. Their method was to mimic the constructions of $\mathbb{C}$ and $\mathbb{H}$ as two-dimensional vector spaces over $\mathbb{R}$ and $\mathbb{C}$, respectively, with multiplication described by a formula similar to multiplication of complex numbers.

This method should bear the names of both Cayley and Graves. Unfortunately, Cayley's work was published first, and his method was later generalized by the American mathematician L. E. Dickson in such papers as [**10**]. As a result, we call this method the *Cayley–Dickson* construction.

Because $\mathbb{O}$ is a normed algebra, by previous reasoning we see that $\mathbb{O}$ is also a division ring, and the table tells us that multiplication in $\mathbb{O}$ is noncommutative. It is also nonassociative, for $o_1(o_2o_3) = o_1o_5 = o_6$, whereas $(o_1o_2)o_3 = o_4o_3 = -o_6$.

The construction of this multiplication table seems quite mysterious; however, if we look more closely, we notice that

$$o_1o_2 = o_4 = -o_2o_1,$$
$$o_2o_3 = o_5 = -o_3o_2,$$
$$o_3o_4 = o_6 = -o_4o_3,$$
$$o_4o_5 = o_7 = -o_5o_4,$$
$$o_5o_6 = o_1 = -o_6o_5,$$
$$o_6o_7 = o_2 = -o_7o_6, \text{ and}$$
$$o_7o_1 = o_3 = -o_1o_7.$$

And now we see it. For distinct $a, b \in \{1, \ldots, 7\}$, $o_ao_b = \pm o_c$, where $\{a, b, c\}$ is one of the seven blocks $D_i$ in the mod 7 (7, 3, 1) block design. The sign is determined by cyclically ordering the blocks as follows: (1, 2, 4), (2, 3, 5), (3, 4, 6), (4, 5, 7), (5, 6, 1), (6, 7, 2), and (7, 1, 3). Then $o_ao_b = o_c$ or $o_ao_b = -o_c$ according as $a$ does or does not directly precede $b$ in the unique ordered block containing $a$ and $b$. Thus, 6 precedes 1 in the block (5, 6, 1), so $o_6o_1 = o_5$; 6 does not directly precede 4 in (3, 4, 6), so $o_6o_4 = -o_3$. (We note that these designated orderings on the blocks of (7, 3, 1) arise as a direct result of Graves' method of constructing $\mathbb{O}$.) And that is why "the multiplication rule for the octonion units" is another name of (7, 3, 1).

But there is more: the octonion algebra has the following structural feature:

1. The octonion algebra $\mathbb{O}$ contains seven complex subalgebras $\mathbb{C}_n = \mathbb{R}\langle o_n\rangle$ and seven quaternion subalgebras $\mathbb{H}_n = \mathbb{R}\langle o_t, o_u, o_v\rangle$, where $\{t, u, v\}$ is a block in (7, 3, 1).
2. Each $\mathbb{H}_n$ contains three of the $\mathbb{C}_k$ and each $\mathbb{C}_k$ is contained in three of the $\mathbb{H}_n$.
3. Each pair $\{\mathbb{C}_k, \mathbb{C}_m\}$ is contained in a unique $\mathbb{H}_n$ together.

In short, $\mathbb{O}$ contains a (7, 3, 1) block design, with the seven quaternion subalgebras as blocks and the seven complex subalgebras as points—another name of (7, 3, 1).

Well, can we do this again and get a 16-squares identity? We applied the Cayley–Dickson construction to the complex numbers to get the quaternions, and the resulting algebra was no longer commutative. We applied Cayley–Dickson to the quaternions to get the octonions and there was a connection with (7, 3, 1), but the resulting algebra was no longer associative. It is natural, therefore, to ask what happens when we apply Cayley–Dickson to the octonions? The answer is that we can do this, and the result is a 16-dimensional real algebra $\mathbb{S}$ called the *sedenions*. The multiplication on $\mathbb{S}$ uses 15 units $\{s_1, \ldots, s_{15}\}$ whose products come from the multiplication table described in FIGURE 6.

| $*$ | $\mathbf{1}$ | $\mathbf{s_1}$ | $\mathbf{s_2}$ | $\mathbf{s_3}$ | $\mathbf{s_4}$ | $\mathbf{s_5}$ | $\mathbf{s_6}$ | $\mathbf{s_7}$ | $\mathbf{s_8}$ | $\mathbf{s_9}$ | $\mathbf{s_{10}}$ | $\mathbf{s_{11}}$ | $\mathbf{s_{12}}$ | $\mathbf{s_{13}}$ | $\mathbf{s_{14}}$ | $\mathbf{s_{15}}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathbf{1}$ | $1$ | $s_1$ | $s_2$ | $s_3$ | $s_4$ | $s_5$ | $s_6$ | $s_7$ | $s_8$ | $s_9$ | $s_{10}$ | $s_{11}$ | $s_{12}$ | $s_{13}$ | $s_{14}$ | $s_{15}$ |
| $\mathbf{s_1}$ | $s_1$ | $-1$ | $s_3$ | $-s_2$ | $-s_5$ | $-s_4$ | $-s_7$ | $s_6$ | $s_9$ | $-s_8$ | $-s_{11}$ | $s_{10}$ | $-s_{13}$ | $s_{12}$ | $s_{15}$ | $-s_{14}$ |
| $\mathbf{s_2}$ | $s_2$ | $-s_3$ | $-1$ | $s_1$ | $s_6$ | $-s_7$ | $s_4$ | $-s_5$ | $s_{10}$ | $s_{11}$ | $-s_8$ | $-s_9$ | $-s_{14}$ | $-s_{15}$ | $s_{12}$ | $s_{13}$ |
| $\mathbf{s_3}$ | $s_3$ | $s_2$ | $-s_1$ | $-1$ | $s_7$ | $-s_6$ | $s_5$ | $-s_4$ | $s_{11}$ | $-s_{10}$ | $s_9$ | $-s_8$ | $-s_{15}$ | $s_{14}$ | $1s_{13}$ | $s_{12}$ |
| $\mathbf{s_4}$ | $s_4$ | $-s_5$ | $-s_6$ | $-s_7$ | $-1$ | $s_1$ | $s_2$ | $s_3$ | $s_{12}$ | $s_{13}$ | $s_{14}$ | $s_{15}$ | $-s_8$ | $-s_9$ | $-s_{10}$ | $-s_{11}$ |
| $\mathbf{s_5}$ | $s_5$ | $s_4$ | $-s_7$ | $s_6$ | $-s_1$ | $-1$ | $-s_3$ | $s_2$ | $s_{13}$ | $-s_{12}$ | $s_{15}$ | $-s_{14}$ | $s_9$ | $-s_8$ | $s_{11}$ | $-s_{10}$ |
| $\mathbf{s_6}$ | $s_6$ | $s_7$ | $s_4$ | $-s_5$ | $-s_2$ | $s_3$ | $-1$ | $-s_1$ | $s_{14}$ | $-s_{15}$ | $-s_{12}$ | $s_{13}$ | $s_{10}$ | $-s_{11}$ | $-s_8$ | $s_9$ |
| $\mathbf{s_7}$ | $s_7$ | $-s_6$ | $s_5$ | $s_4$ | $-s_3$ | $-s_2$ | $s_1$ | $-1$ | $s_{15}$ | $s_{14}$ | $-s_{13}$ | $-s_{12}$ | $s_{11}$ | $s_{10}$ | $-s_9$ | $-s_8$ |
| $\mathbf{s_8}$ | $s_8$ | $-s_9$ | $-s_{10}$ | $-s_{11}$ | $-s_{12}$ | $-s_{13}$ | $-s_{14}$ | $-s_{15}$ | $-1$ | $s_1$ | $s_2$ | $s_3$ | $s_4$ | $s_5$ | $s_6$ | $s_7$ |
| $\mathbf{s_9}$ | $s_9$ | $s_8$ | $-s_{11}$ | $s_{10}$ | $-s_{13}$ | $s_{12}$ | $s_{15}$ | $-s_{14}$ | $-s_1$ | $-1$ | $-s_3$ | $s_2$ | $-s_5$ | $s_4$ | $s_7$ | $-s_6$ |
| $\mathbf{s_{10}}$ | $s_{10}$ | $s_{11}$ | $s_8$ | $-s_9$ | $-s_{14}$ | $-s_{15}$ | $s_{12}$ | $s_{13}$ | $-s_2$ | $s_3$ | $-1$ | $-s_1$ | $-s_6$ | $-s_7$ | $s_4$ | $s_5$ |
| $\mathbf{s_{11}}$ | $s_{11}$ | $-s_{10}$ | $s_9$ | $s_8$ | $-s_{15}$ | $s_{14}$ | $-s_{13}$ | $s_{12}$ | $-s_3$ | $-s_2$ | $-s_1$ | $-1$ | $-s_7$ | $s_6$ | $-s_5$ | $s_4$ |
| $\mathbf{s_{12}}$ | $s_{12}$ | $s_{13}$ | $s_{14}$ | $s_{15}$ | $s_8$ | $-s_9$ | $-s_{10}$ | $-s_{11}$ | $-s_4$ | $s_5$ | $s_6$ | $s_7$ | $-1$ | $-s_1$ | $-s_2$ | $-s_3$ |
| $\mathbf{s_{13}}$ | $s_{13}$ | $-s_{12}$ | $s_{15}$ | $-s_{14}$ | $s_9$ | $s_8$ | $s_{11}$ | $-s_{10}$ | $-s_5$ | $-s_4$ | $s_7$ | $-s_6$ | $s_1$ | $-1$ | $s_3$ | $-s_2$ |
| $\mathbf{s_{14}}$ | $s_{14}$ | $-s_{15}$ | $-s_{12}$ | $s_{13}$ | $s_{10}$ | $-s_{11}$ | $s_8$ | $s_9$ | $-s_6$ | $-s_7$ | $-s_4$ | $s_5$ | $s_2$ | $-s_3$ | $-1$ | $s_1$ |
| $\mathbf{s_{15}}$ | $s_{15}$ | $s_{14}$ | $-s_{13}$ | $-s_{12}$ | $s_{11}$ | $s_{10}$ | $-s_9$ | $s_8$ | $-s_7$ | $s_6$ | $-s_5$ | $-s_4$ | $s_3$ | $s_2$ | $-s_1$ | $-1$ |

**Figure 6** The sedenions

It happens that there are 15 eight-dimensional subalgebras of $\mathbb{S}$, each isomorphic to the octonions, and for each of these, the multiplication tables are generated by 15 isomorphic copies of (7, 3, 1). One obtains the overall multiplication by adjusting the tables of the 15 octonions to achieve consistency of the products from one octonion subalgebra to the next. There are also 35 four-dimensional subalgebras of $\mathbb{S}$, each isomorphic to the quaternions, and 15 two-dimensional subalgebras of $\mathbb{S}$, each isomorphic to the complex numbers. And there is another design hidden within this set of subalgebras. Namely, the 15 complex subalgebras (points) and the 35 quaternionic subalgebras (blocks) form a (15, 35, 7, 3, 1) block design.

However, the string of normed algebras—that is, algebras with sums-of-squares identities—stops with $\mathbb{O}$. The reason is that $\mathbb{S}$ contains pairs of nonzero elements whose product equals zero, and this prevents $\mathbb{S}$ from being a normed algebra. Indeed, suppose there were a norm $N$ on $\mathbb{S}$. From the table we see that

$$(s_5 + s_9)(s_7 - s_{11}) = s_5s_7 + s_9s_7 - s_5s_{11} - s_9s_{11} = 0.$$

Thus, $0 = N(0) = N((s_5 + s_9)(s_7 - s_{11})) = N(s_5 + s_9)N(s_7 - s_{11})$, so one of $N(s_5 + s_9)$, $N(s_7 - s_{11})$ must be 0. But this implies that either $s_5 = -s_9$ or $s_7 = s_{11}$, neither of which holds. Hence, the sedenions are not a normed algebra. Finally, the Cayley–Dickson operation on $\mathbb{S}$ won't produce a normed algebra, as the resulting 32-dimensional algebra would contain 31 copies of $\mathbb{S}$. Thus, there are no more real normed algebras to be produced by the Cayley–Dickson construction, and so—according to L. E. Dickson's modification of Hurwitz' original proof [**10**]—there are no real normed algebras beyond the octonions.

And with that, our journey through more of the many names of (7, 3, 1) is done.

## REFERENCES


1. J. C. Baez, The octonions, *Bull. Amer. Math. Soc.* **39** (2002) 145–205, see also http://math.ucr.edu/home/baez/octonions/oct.pdf.
2. T. Beth, D. Jungnickel, H. Lenz, *Design Theory*. Second edition. Cambridge Univ. Press, Cambridge, 1999.
3. R. C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics* **9** (1939) 353–399.
4. E. Brown, The many names of (7, 3, 1), *Math. Mag.* **75** (2002) 83–94.
5. E. Brown, N. Loehr, Why is PSL(2, 7) ≅ GL(3, 2)?, *Amer. Math. Monthly* **116** no. 8 (October 2009) 727–731.
6. E. Brown, K. Mellinger, Kirkman's Schoolgirls wearing hats and walking through fields of numbers, *Math. Mag.* **82** (2009) 3–15.
7. *Handbook of Combinatorial Designs*. Second edition. Ed. by C. J. Colbourn and J. H. Dinitz. Chapman and Hall/CRC, Boca Raton FL, 2007.
8. C. Mulcahy, *Mathematical Card Magic: Fifty-Two New Effects*. A K Peters/CRC, Boca Raton FL, 2013.
9. J. H. Conway, D. A. Smith, *On Quaternions and Octonions*. A K Peters, Natick MA, 2003.
10. L. E. Dickson, On quaternions and their generalizations and the history of the eight square theorem, *Annals of Math.* second series, **20** (1919) 155–171.
11. R. Guy, The unity of combinatorics, *Combinatorics Advances*. Edited by C. J. Colbourn and E. S. Mahmoodian. Kluwer Academic Publishers, Dordrecht, The Netherlands. 1995, pp. 129–159.
12. M. Hall, Jr., *Combinatorial Theory*. Second edition. John Wiley & Sons, New York, 1986.
13. William R. Hamilton, Letter from Sir W. R. Hamilton to Rev. Archibald H. Hamilton, August 5, 1865.
14. T. P. Kirkman, On a problem in combinations, *Camb. Dublin Math. J.* **2** (1847) 191–204.
15. T. P. Kirkman, Query 6, *Lady's and Gentlemen's Diary* (1850) p. 48.
16. T. P. Kirkman, Note on an unanswered prize question, *Camb. Dublin Math. J.* **5** (1850) 255–262.
17. C. E. Shannon, A mathematical theory of communication, *Bell System Tech. J.* **27** (1948) 379–423, 623–656.
18. J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938) 377–385.
19. T. M. Thompson, *From Error-Correcting Codes through Sphere Packings to Simple Groups*. Carus Mathematical Monograph No. 21. Mathematical Association of America, Washington, DC, 1983.
20. W. D. Wallis, *Introduction to Combinatorial Designs*. Second edition. Chapman and Hall/CRC, Boca Raton FL, 2007.
21. W. S. B. Woolhouse, Prize question 1733, *Lady's and Gentleman's Diary*, 1844.


**Summary.** The (7, 3, 1) block design is an object that shows up in many areas of mathematics. In fact, (7, 3, 1) seems to appear again and again in unexpected places. A 2002 paper described (7, 3, 1)'s connection with such areas as graph theory, number theory, topology, round-robin tournaments, and algebraic number fields.

In this paper, we show how (7, 3, 1) makes appearances in the areas of error-correcting codes, $n$-dimensional finite projective geometries, difference sets, normed algebras, and the three-circle Venn diagram.

**EZRA (BUD) BROWN** (MR Author ID: 222489) grew up in New Orleans and has degrees from Rice University and Louisiana State University. He has been at Virginia Tech since 1969, where he is currently Alumni Distinguished Professor of Mathematics. His research interests include number theory and combinatorics. In graduate school, he first met the (7, 3, 1) block design, and the design continues to amaze him with its many and varied mathematical connections. He is a frequent contributor to the MAA journals.

In his spare time, Bud enjoys singing (from opera to rock and roll), playing jazz piano, and solving word puzzles. He and his wife, Jo, enjoy kayaking, bicycling, and birding. He occasionally bakes biscuits for his students, and he once won a karaoke contest.