The Fabulous (11, 5, 2) Biplane

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

——To Annette L. Brown: Pianist, Mother, Grandmother, and Great-Grandmother *extraordinaire*.

After a workshop for new teaching assistants on innovations in teaching, a new sociology graduate student wandered into my office and asked the question, "Tell me ... how do you make math exciting for students?" By chance, I just happened to have on my computer screen a picture that exhibits some of the symmetries of one of the most intriguing objects in mathematics: the (11, 5, 2) biplane.

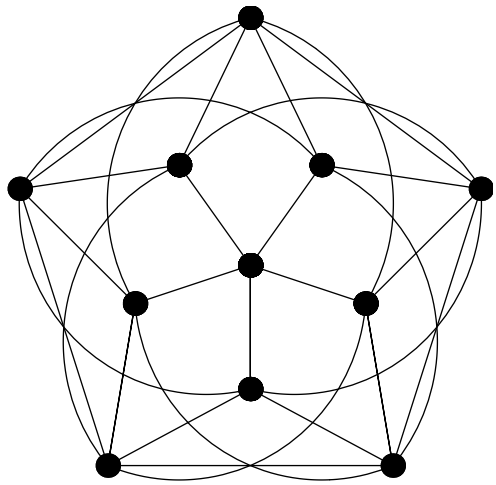

Figure 1 A fascinating picture

I told him of my chagrin on seeing a picture similar to FIGURE 1 (but much prettier, and in color) on the cover of a book [**6**] on combinatorial designs. The picture was lovely, and the reason for my strong feelings was purely selfish: I was trying to construct such a picture, and somebody else thought of it first.

But it wasn't labeled.

It was fun finding a labeling compatible with the symmetries of the biplane. To find generators for the symmetry group of the biplane—which turns out to have a name, $PSL(2, 11)$—was more fun. The best part, however, was learning about the exact connection between the biplane and six pairs of mathematical objects.

We find these six mathematical pairs just outside the boundaries of many traditional courses, where a bit of exploration can lead the curious to all manner of interesting mathematics. A good course in coding theory will mention two pairs of perfect error-correcting codes, namely the Golay codes $\{G_{11}, G_{12}\}$ and $\{G_{23}, G_{24}\}$, but sometimes only in passing. Look past the usual topics in combinatorics into the world of combinatorial designs and you will meet two pairs of Steiner systems, namely $\{S(4, 5, 11), S(5, 6, 12)\}$ and $\{S(4, 7, 23), S(5, 8, 24)\}$. Beyond the first course

in group theory lie two pairs of finite simple groups, namely the Mathieu groups $\{M_{11}, M_{12}\}$ and $\{M_{23}, M_{24}\}$. It was quite a revelation to learn just how these codes, designs, and groups connect with the biplane and with each other.

I told the student all about this, including the reason that the biplane is called a biplane, and he loved it; maybe you will, too.

Difference sets, block designs, and biplanes

The (11, 5, 2) biplane is a collection of the following eleven 5-element subsets of $\{1, 2, 3, 4, 5, 6, 7, 8, 9, X, 0\}$ (we think of X as 10, and we have written $abcde$ for the set $\{a, b, c, d, e\}$:

$$\begin{array}{llll} B_1 = 13459 & B_2 = 2456X & B_3 = 35670 & B_4 = 46781 \\ B_5 = 57892 & B_6 = 689X3 & B_7 = 79X04 & B_8 = 8X015 \\ B_9 = 90126 & B_X = X1237 & B_0 = 02348 & \end{array}$$

The (11, 5, 2) biplane

This is an example of a *block design*, which is an arrangement of v objects called *varieties* into b sets called *blocks*. Each variety appears in exactly r blocks, each block contains exactly k varieties, and each pair of varieties appears together in exactly λ blocks. From the above, we see that $b = v = 11$ and $k = 5$. It is a bit less obvious that $r = 5$ and still less obvious that $\lambda = 2$: for example, 1 appears in blocks B_1, B_4, B_8, B_9, and B_X, and 7 and 0 appear together in blocks B_3 and B_7.

Block designs first appeared in the 1930s in connection with the design of certain agricultural experiments, although they are implicit in the work of Woolhouse [**13**] and Kirkman [**7**] as early as 1844 and 1847, respectively. (These papers are hard to find; a more recent reference is Richard Guy's excellent survey article [**4**].) The parameters b, v, r, k, and λ are not independent: it happens that $bk = vr$ and $r(k-1) = \lambda(v-1)$. Thus, if $b = v$, then $r = k$ and we speak of a (v, k, λ) *symmetric design*. Hence, the (11, 5, 2) biplane is an (11, 5, 2) symmetric design, which explains the numerical part of its name.

Symmetric designs also have the feature that two distinct blocks intersect in exactly λ varieties; for a proof, see Hall [**5**, Section 10.2].

A closer look reveals that we may construct the entire (11, 5, 2) biplane from B_1 by adding a particular integer mod 11 to each element; for example, if we add 5 to each element of B_1 and reduce the results mod 11, we find that

$$\{1+5, 3+5, 4+5, 5+5, 9+5\} \equiv \{6, 8, 9, X, 3\} \equiv B_6 \bmod 11.$$

Now, B_1 is an example of a *difference set*; that is, every nonzero integer mod 11 appears exactly twice among the 20 differences $i - j$ mod 11 for i and j distinct elements of B_1 (in the following, $a \equiv b$ is short for $a \equiv b$ mod 11):

$$\begin{array}{lll} \mathbf{1} \equiv 4-3 \equiv 5-4 & \mathbf{2} \equiv 3-1 \equiv 5-3 & \mathbf{3} \equiv 4-1 \equiv 1-9 \\ \mathbf{4} \equiv 5-1 \equiv 9-5 & \mathbf{5} \equiv 9-4 \equiv 3-9 & \mathbf{6} \equiv 9-3 \equiv 4-9 \\ \mathbf{7} \equiv 1-5 \equiv 5-9 & \mathbf{8} \equiv 9-1 \equiv 1-4 & \mathbf{9} \equiv 1-3 \equiv 3-5 \\ & \mathbf{10} \equiv 3-4 \equiv 4-5. & \end{array}$$

More generally, a (v, k, λ) *difference set* is a k-element subset S of $V = \{0, 1, \ldots, v-1\}$ such that every nonzero integer mod v can be written in exactly λ ways as a difference of elements of S. So, the set $\{1, 3, 4, 5, 9\}$ of nonzero perfect squares mod 11 is an (11, 5, 2) difference set.

In fact, for every prime $p \equiv 3 \bmod 4$, the set Q_p of nonzero perfect squares mod p is a $(p, (p-1)/2, (p-3)/4)$ difference set (a proof appears in [**2**]). For example, you can check that $Q_{23} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$ is a $(23, 11, 5)$ difference set. (Exercise: Find the five different ways to write 7 as a difference of elements of Q_{23}.)

What is interesting here is that every difference set gives rise to a symmetric design in the following way:

THEOREM 1. *Let* $D = \{x_1, x_2, \ldots, x_k\}$ *be a* (v, k, λ) *difference set. Let* $D_i := \{x_1 + i, \ldots, x_k + i\}$ *where addition is* mod v. *Then the* v *sets* $D_0, \ldots, D_{v-1}$ *are the blocks of a* (v, k, λ) *symmetric design.*

(For a proof, see Hall [**5**, Theorem 11.1.1].) Thus, the $(11, 5, 2)$ difference set gives rise to the $(11, 5, 2)$ symmetric design.

Symmetric designs with $\lambda = 1$ have the property that every pair of varieties determines a unique block and every pair of blocks intersects in a unique variety. Reading *line* for *block* and *point* for *variety* gives us the first two axioms of projective geometry; for this reason, $(v, k, 1)$ designs are called *finite projective planes*, or planes for short. Now for a $(v, k, 2)$ design, every pair of varieties determines exactly two blocks and every pair of blocks intersects in exactly two varieties. For this reason, the blocks and varieties of a $(v, k, 2)$ design are called lines and points, respectively, and the designs themselves are called *biplanes*—and that explains the second part of the $(11, 5, 2)$ biplane's name.

As stated earlier, part of my fascination with the $(11, 5, 2)$ biplane lies both in its symmetries and in the challenge of drawing a picture that will reveal some of its symmetries. By a symmetry of a design, we mean a permutation of the varieties that simultaneously permutes the blocks. For any design, the set of all such permutations is a group called the *automorphism group* of the design. So, first we'll talk about permutations and automorphism groups, and then we'll draw another picture.

The automorphism group of the biplane

A *permutation* on a set Y is a mapping of the set to itself that is one-to-one and onto. An *n-cycle* is an expression of the form $(a_1\ a_2 \ldots a_n)$, where the a_i are distinct. The cycle notation is a standard way to describe permutations on finite sets; here is an example to show how it works. If we write $f = (1\ 3\ 6)(4\ 5)$, it means that $f(1) = 3$, $f(3) = 6$, $f(6) = 1$, $f(4) = 5$, $f(5) = 4$, and $f(x) = x$ for all $x \notin \{1, 3, 4, 5, 6\}$; in this notation, 1-cycles are frequently omitted. In this example, we say that f is a product of two disjoint cycles. Similarly, $g = (1\ 2)$ means that g switches 1 and 2 and leaves everything else fixed. Since permutations are functions, they compose from right to left. If we denote composition by $\circ$, then $f \circ g = (1\ 3\ 6)(4\ 5)(1\ 2)$. This maps 1 to 2, 2 to 3 (since $g(2) = 1$ and $f(1) = 3$), 3 to 6, 4 to 5, 5 to 4, and 6 to 1. We see that $f \circ g = (1\ 2\ 3\ 6)(4\ 5)$ as a product of disjoint cycles.

Let $\mathcal{D}$ be a block design. An *automorphism* of $\mathcal{D}$ is a permutation f of the set V of varieties that is simultaneously a permutation of the set B of blocks. (We say that f *induces* a permutation on B.) For example, the permutation $\tau = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ X\ 0)$ of the set $V = \{1, 2, 3, 4, 5, 6, 7, 8, 9, X, 0\}$ of varieties induces the permutation $\tau' = (B_1\ B_2\ B_3\ B_4\ B_5\ B_6\ B_7\ B_8\ B_9\ B_X\ B_0)$ of the corresponding set of blocks. The set of all such automorphisms is a group under composition, called the *automorphism group* $Aut(\mathcal{D})$ of the design $\mathcal{D}$.

It turns out that there are 660 automorphisms of the $(11, 5, 2)$ biplane. How do we find them all?

In some sense, the automorphism τ is an obvious choice, for the blocks of the biplane were created by repeatedly adding 1 (mod 11) to each member of the difference set $B_1 = \{1, 3, 4, 5, 9\}$. It is not so obvious that the permutation $\mu = (1\ 3\ 9\ 5\ 4)(2\ 6\ 7\ X\ 8)(0)$ also induces a permutation of the blocks—but it does, namely $\mu' = (B_2\ B_4\ B_X\ B_6\ B_5)(B_0\ B_9\ B_3\ B_7\ B_8)(B_1)$.

Clearly, we need a systematic way to find the rest of the automorphisms. We make a four-fold application of that useful and elegant result, the Orbit-Stabilizer Theorem. But first, we need a couple of definitions. Suppose that G is a group of permutations on the set S, let $g \in G$, and let $T \subseteq S$. Then $g(T)$ is the set of images $g(t)$ for all $t \in T$; an element $g \in G$ leaves T *setwise fixed* if $g(T) = T$. The *stabilizer* of T in G, $Stab_G(T)$, is the set of all permutations g in G that leave T setwise fixed. The *orbit* of T, $Orb_G(T)$, is the set of all $Y \subseteq S$ for which $Y = g(T)$ for some permutation $g \in G$. (If $T = \{t\}$, we customarily write $Stab_G(t)$ and $Orb_G(t)$, ignoring the braces.) Let $|A|$ be the number of elements in the set A. Here is the theorem, which follows from the definition of a permutation and from Lagrange's Theorem:

THEOREM 2. (THE ORBIT-STABILIZER THEOREM) *Let G be a finite group of permutations of a set S and let $T \subseteq S$. Then* (a) *$Stab_G(T)$ is a subgroup of G, and* (b) $|G| = |Stab_G(T)| \cdot |Orb_G(T)|$.

We now define the groups G, H, K, and L as follows:

$$\begin{aligned} G &= Aut((11, 5, 2)); \\ H &= Stab_G(B_1) = \{\text{automorphisms in } G \text{ that leave } B_1 \text{ setwise fixed}\}; \\ K &= Stab_H(1) = \{\text{automorphisms in } H \text{ that leave 1 fixed}\}; \\ L &= Stab_K(3) = \{\text{automorphisms in } K \text{ that leave 3 fixed}\}. \end{aligned} \tag{1}$$

By the Orbit-Stabilizer Theorem, L, K, and H are subgroups of K, H, and G, respectively, and since $4 \in B_1$, we see that

$$\begin{aligned} |G| &= |H| \cdot |Orb_G(B_1)| = |K| \cdot |Orb_H(1)| \cdot |Orb_G(B_1)| \\ &= |L| \cdot |Orb_K(3)| \cdot |Orb_H(1)| \cdot |Orb_G(B_1)| \\ &= |Stab_L(4)| \cdot |Orb_L(4)| \cdot |Orb_K(3)| \cdot |Orb_H(1)| \cdot |Orb_G(B_1)|. \end{aligned} \tag{2}$$

If we can show that $|Stab_L(4)| = 1$, $|Orb_L(4)| = 3$, $|Orb_K(3)| = 4$, $|Orb_H(1)| = 5$, and $|Orb_G(B_1)| = 11$, it will follow that $|G| = 1 \cdot 3 \cdot 4 \cdot 5 \cdot 11 = 660$. Let's call it a theorem:

THEOREM 3. *Let G, H, K, and L be as defined above.* (a) *If $\sigma \in H$ and σ fixes 1, 3, and 4, then $\sigma = I$, the identity map, and $|Stab_L(4)| = 1$.* (b) *$|Orb_L(4)| = 3$, $|Orb_K(3)| = 4$, $|Orb_H(1)| = 5$, and $|Orb_G(B_1)| = 11$.* (c) *$|G| = 660$.*

Proof.

(a) Since $\sigma \in H$, σ fixes B_1 setwise. Now, σ might permute some of the other blocks. We can show that this is false by seeing how it permutes the blocks containing the pairs $\{1, 4\}$, $\{1, 3\}$, and $\{3, 4\}$. Since $B_4 = 46781$, $B_X = X1237$, and $B_0 = 02348$ are the only other blocks containing those pairs, it follows that σ fixes the sets B_4, B_X, and B_0. Thus, σ fixes the subsets $\{6, 7, 8\}$, $\{X, 2, 7\}$, and $\{0, 2, 8\}$ of B_4, B_X, and B_0, respectively. The only way this can happen is if σ fixes the elements 2, 7, and 8. As a consequence, σ also fixes 6, X, and 0, and hence σ fixes

$B_3 = 35670$. It follows that σ fixes 5. Finally, since σ fixes B_1, it must also fix 9, and we conclude that $\sigma = I$, and so $|Stab_L(4)| = 1$.

(b) Let $L = Stab_K(3)$ and let $\alpha \in L$. Then α fixes 1 and 3. The method in (a) shows that any permutation that fixes three distinct points must be the identity map. Hence, either $\alpha = I$ or α cyclically permutes 4, 5, and 9. A little work shows that either α or α^{-1} is equal to $(4\ 5\ 9)(2\ 7\ X)(0\ 6\ 8)$. It follows that $Orb_L(4) = \{4, 5, 9\}$, and so $|Orb_L(4)| = 3$. A similar argument shows that $K = Stab_H(1)$ contains the permutations I, $\beta = (3\ 4)(5\ 9)(2\ 8)(6\ X)$, $\gamma = (3\ 5)(4\ 9)(2\ 8)(7\ 0)$, and $\beta \circ \gamma$; it follows that $Orb_K(3) = \{3, 4, 5, 9\}$, and so $|Orb_K(3)| = 4$. Next, $H = Stab_H(1)$ contains the powers of $\mu = (1\ 3\ 9\ 5\ 4)(2\ 6\ 7\ X\ 8)$. It follows that $Orb_H(1) = \{1, 3, 4, 5, 9\}$, and so $|Orb_H(1)| = 5$. Finally, G contains the powers of $\tau = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ X\ 0)$; the kth powers of the induced permutation τ' send B_1 to B_k for each k. Hence, $Orb_G(B_1)$ contains all eleven blocks, and we conclude that $|Orb_G(B_1)| = 11$.

(c) We now put the pieces together. By the Orbit-Stabilizer Theorem and Equation (2), we see that

$$\begin{aligned} |G| &= |Stab_L(4)| \cdot |Orb_L(4)| \cdot |Orb_K(1)| \cdot |Orb_H(1)| \cdot |Orb_G(B_1)| \\ &= 1 \cdot 3 \cdot 4 \cdot 5 \cdot 11 = 660, \end{aligned}$$

and we are done. ∎

With so much symmetry, there ought to be a picture that tells us something about the (11, 5, 2) biplane, and FIGURE 1 is where this all began. So let's look at FIGURE 1 with more experienced eyes.

Symmetries of the biplane as revealed in pictures

"Draw a figure." So said that master problem-solver and teacher, George Pólya, in his classic "How To Solve It" [**10**]. We learn so much from figures, so we follow Pólya's lead and return to the picture in FIGURE 1. As we mentioned earlier, the context suggested that it was a picture of the (11, 5, 2) biplane. It is clear that FIGURE 1 is a dressed-up regular pentagon. As such, it is setwise fixed by both a 1/5-turn about the center and reflections about lines through the center. The challenge was to label the figure so that these geometric motions corresponded to symmetries of the (11, 5, 2) biplane, and my efforts were eventually rewarded. In FIGURE 2, the clockwise 1/5-turn about the point 0 and the reflection about the line through 0 and 7 correspond to the automorphisms μ and ρ, respectively, where $\mu = (1\ 3\ 9\ 5\ 4)(2\ 6\ 7\ X\ 8)$ and $\rho = (2\ 8)(3\ 4)(5\ 9)(6\ X)$.

Let us now see just how the figure depicts these automorphisms.

First, consider $\mu = (1\ 3\ 9\ 5\ 4)\ (2\ 6\ 7\ X\ 8)$. As mentioned above, μ induces the permutation $\mu' = (B_2\ B_4\ B_X\ B_6\ B_5)\ (B_0\ B_9\ B_3\ B_7\ B_8)$ on the blocks of the biplane.

Now, look at FIGURE 2. The exterior pentagon joins the five points labeled 1, 3, 9, 4, and 5. This is the block B_1, which is mapped into itself by a 1/5-turn about 0. Next, the dotted lines connect the five points labeled 4, 8, 0, 2, and 3. This is just the block $B_0 = 02348$, and if we rotate the figure about 0 by a 1/5-turn, we see that B_0 is mapped into $B_9 = \{1, 2, 0, 6, 9\}$, B_9 into $B_3 = \{3, 6, 0, 7, 5\}$, B_3 into $B_7 = \{9, 7, 0, X, 4\}$, B_7 into $B_8 = \{5, X, 0, 8, 1\}$, and B_8 into B_0. Finally, the bold lines connect the five points labeled 2, 9, 7, 5 and 8. This is the block $B_5 = \{5, 7, 8, 9, 2\}$, and if we rotate the figure about 0 by a 1/5-turn, we see that B_5 is mapped into $B_2 = \{6, 5, X, 4, 2\}$,

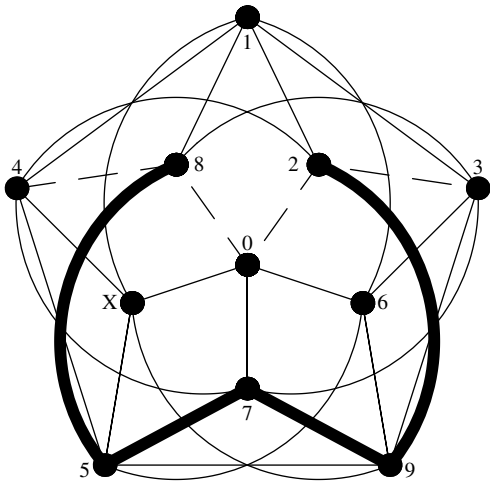

Figure 2 The fabulous (11, 5, 2) biplane

B_2 into $B_4 = \{7, 4, 8, 1, 6\}$, B_4 into $B_X = \{X, 1, 2, 3, 7\}$, B_X into $B_6 = \{8, 3, 6, 9, X\}$, and B_6 into B_5.

Thus, the 1/5-turn about 0 induces the permutation

$$(B_2\ \ B_4\ \ B_X\ \ B_6\ \ B_5)(B_0\ \ B_9\ \ B_3\ \ B_7\ \ B_8)(B_1)$$

on the blocks of the biplane. But μ' is exactly this permutation! As for ρ, you can show that the reflection about the line through 0 and 7 induces

$$(B_2\ \ B_6)(B_4\ \ B_X)(B_3\ \ B_7)(B_8\ \ B_9)(B_0)(B_1)(B_7) = \rho'.$$

Are there ways to draw the (11, 5, 2) biplane that exhibit symmetries other than μ, ρ and others of orders 5 and 2? It is an interesting exercise to find one that exhibits the symmetry of $\alpha = (4\ \ 5\ \ 9)(2\ \ 7\ \ X)(0\ \ 6\ \ 8)$ and has order 3.

We are almost ready to talk about the mathematical pairs connected to the (11, 5, 2) biplane. The most direct path to these pairs leads through a certain matrix associated with the (11, 5, 2) biplane, called the incidence matrix.

One way to describe a block design is by its *incidence matrix*, a $b \times v$ matrix whose (i, j)th entry is 1 or 0 according as the ith block does or does not contain the jth variety. Here is the incidence matrix $\mathbf{M}$ for the (11, 5, 2) symmetric design. The rows correspond to the blocks in the above order, and the columns correspond to the varieties in the order 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X:

$$\mathbf{M} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

As we shall soon see, the matrix $\mathbf{M}$ is instrumental in constructing the two pairs of Golay codes $\{G_{11}, G_{12}\}$ and $\{G_{23}, G_{24}\}$. So, let's talk about error-correcting codes.

Error-correcting codes

Mathematical schemes to deal with signal errors first appeared in the 1940s in the work of several researchers, including Claude Shannon, Richard Hamming, and Marcel Golay. People at various research labs saw the need for devices that would automatically detect and correct errors in signal transmissions across noisy channels. What they came up with was 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 n-long strings called *blocks*, to be taken from a fixed alphabet of size q; a particular set of such blocks, or *codewords*, is called a *q-ary code of length n*. If q is a prime number, then a q-ary code of length n is called *linear* if the codewords form a subspace of $\mathbb{Z}_q^n$, the n-dimensional vector space over $\mathbb{Z}_q$, the integers mod q. To *correct* errors means to determine the intended codeword when one has been received incorrectly. 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 $D(1101000, 0011010) = 4$. If I send the block v and you receive the block w, then $D(v, w)$ errors occurred while sending v.

It follows that if the words in a code are all sufficiently 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.

One way to transmit bits is to send each bit three times, so that our only codewords are 000 and 111. If you receive 010, then it is most likely that I sent 000 and so the intended message was 0; this is the triplication or majority-vote code. Thus, 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.

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. (Exercise: Show that a code with minimum distance 5 will detect up to 4 errors and correct up to 2. You can then 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.) For an (n, k) code to be efficient, the ratio k/n should be as large as possible, consistent with its error detection and correction capabilities. Maximum efficiency in an (n, k) m-error correcting code occurs when it can correct up to m errors, and no others. Such a code is called *perfect*. Here is a very nice necessary condition—which we can verify—for the existence of a perfect code:

THEOREM 4. *If there exists a q-ary (n, k) perfect m-error-correcting code, then*

$$1 + (q-1)n + (q-1)^2\binom{n}{2} + \cdots + (q-1)^m\binom{n}{m} = q^r$$

for some positive integer r, and $k = n - r$.

Proof. A codeword of length n can have a single error occur in n positions, two errors in $\binom{n}{2}$ positions, and in general m errors in $\binom{n}{m}$ ways. For a q-ary code, there are

$q-1$ ways for a single error to occur at a given position, $(q-1)^2$ ways for two errors to occur at two given positions, and in general $(q-1)^m$ ways for m errors to happen at m given positions. Thus, the total number of ways in which no more than m errors can occur relative to a given codeword is equal to

$$1+(q-1)n+(q-1)^2\binom{n}{2}+\cdots+(q-1)^m\binom{n}{m}. \tag{3}$$

To complete the proof, we need to recognize this as a power of q.

The set of all n-long q-ary strings differing from a given codeword W in at most m positions is called the *sphere of radius m about W*. If a code is perfect, then every n-string lies in a sphere of radius m about some codeword, and the spheres do not overlap. That is, the union of the spheres is equal to the entire space of n-tuples. Since the latter has size q^n, it follows that

$$(\text{number of } m\text{-spheres}) \cdot (\text{size of each } m\text{-sphere}) = q^n.$$

Thus, since q is a prime, the size of an m-sphere must be a power of q, say, q^r, and (3) is satisfied. Finally, every m-sphere is centered about one of the q^k codewords. Since $q^n = q^r \cdot q^k$, it follows that $k = n-r$, and we are done. ∎

Now, 11 happens to be the smallest prime number p for which 2^p-1 is not a prime. For $p = 2$, 3, 5, and 7, we obtain the primes $2^p-1 = 3$, 7, 31, and 127, and $2^{11}-1 = 2047 = 23\cdot 89$ is composite. But there is ample recompense for the failure of $2^{11}-1$ to be prime; let's take a closer look:

$$\begin{aligned} 2^{11} &= 1+23\cdot 89 \\ &= 1+23(1+11+11\cdot 7) \\ &= 1+23+23\cdot 11+23\cdot 11\cdot 7 \\ &= 1+23+\binom{23}{2}+\binom{23}{3}. \end{aligned}$$

In 1949, Golay noted that this is precisely the case $q=2, n=23, r=11$ of Theorem 4. That is, the necessary condition for the existence of a binary $(23, 23-11)$ perfect 3-error-correcting code is satisfied.

In the same year, he also noticed that

$$1+2\cdot 11+2^2\binom{11}{2} = 1+22+220 = 243 = 3^5,$$

so that the necessary condition for the existence of a ternary $(11, 11-5)$ perfect 2-error-correcting code is satisfied.

Of course, necessary conditions are not always sufficient, but in 1949, Golay constructed two linear codes with the above parameters and two slightly larger linear codes. The binary codes are G_{23} and G_{24}, the (23, 12) Golay code and the (24, 12) extended Golay code; the ternary codes are G_{11} and G_{12}, the (11, 6) Golay code and the (12, 6) extended Golay code.

We can describe an $(n, n-r)$ q-ary linear code as the row space of a matrix of n columns and rank r over $\mathbb{Z}_q$, the so-called *generating matrix* of the code. Let $\mathbf{A}$ be the following 12×24 binary matrix:

$$\mathbf{A} = \left[\begin{array}{cccccccccccc|cccccccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&0&0&0&1&\mathbf{0}\\
0&1&0&0&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&0&0&0&\mathbf{1}\\
0&0&1&0&0&0&0&0&0&0&0&0&1&1&0&1&1&0&1&1&1&0&0&\mathbf{0}\\
0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&0&1&1&0&1&1&1&0&\mathbf{0}\\
0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&\mathbf{0}\\
0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&1&1&0&1&1&\mathbf{1}\\
0&0&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&1&0&1&1&0&1&\mathbf{1}\\
0&0&0&0&0&0&0&1&0&0&0&0&1&1&1&0&0&0&1&0&1&1&0&\mathbf{1}\\
0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&1&0&0&0&1&0&1&1&\mathbf{0}\\
0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&1&1&0&0&0&1&0&1&\mathbf{1}\\
0&0&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&0&0&0&1&0&\mathbf{1}\\
0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&1&1&1&1&1&1&1&\mathbf{1}
\end{array}\right] \tag{4}$$

A is a generating matrix for G_{24}; deleting its last (boldface) column gives a generating matrix for G_{23}.

G_{12} is the row space of the following 12×12 ternary matrix **B**, and G_{11} is the row space of B', obtained from **B** by deleting the last column.

$$\mathbf{B} = \left[\begin{array}{cccccccccccc}
-1&1&1&-1&1&1&1&-1&-1&-1&1&\mathbf{-1}\\
-1&-1&1&1&-1&1&1&1&-1&-1&-1&\mathbf{1}\\
-1&1&-1&1&1&-1&1&1&1&-1&-1&\mathbf{-1}\\
-1&-1&1&-1&1&1&-1&1&1&1&-1&\mathbf{-1}\\
-1&-1&-1&1&-1&1&1&-1&1&1&1&\mathbf{-1}\\
-1&-1&-1&-1&1&-1&1&1&-1&1&1&\mathbf{1}\\
-1&1&-1&-1&-1&1&-1&1&1&-1&1&\mathbf{1}\\
-1&1&1&-1&-1&-1&1&-1&1&1&-1&\mathbf{1}\\
-1&1&1&1&-1&-1&-1&1&-1&1&1&\mathbf{-1}\\
-1&-1&1&1&1&-1&-1&-1&1&-1&1&\mathbf{1}\\
-1&1&-1&1&1&1&-1&-1&-1&1&-1&\mathbf{1}\\
-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&\mathbf{-1}
\end{array}\right]$$

Note that these codes are 6-dimensional subspaces of $\mathbb{Z}_3^{12}$ and $\mathbb{Z}_3^{11}$, respectively, since **B** and $\mathbf{B}'$ have rank six. (Arithmetic in $\mathbb{Z}_3$ is just arithmetic mod 3 with the symbols -1, 0 and 1.)

We are now ready to connect the (11, 5, 2) biplane with the Golay code pairs. Let **U** and **V** be the upper rightmost 11×11 submatrices of **A** and **B**, respectively.

Take **U** and change all the 1s on the main diagonal to 0s, and what do you get? You get **M**, the incidence matrix for the (11, 5, 2) biplane.

Take **V** and change all the -1s to 0s. Then, change all the 1s on the main diagonal to 0s, and what do you get? Again, you get **M**.

Thus, from the (11, 5, 2) biplane we are able to construct the pair of binary Golay codes G_{23} and G_{24} and the pair of ternary Golay codes G_{11} and G_{12}.

Nice connections, to be sure, and there are even more connections with Steiner systems, so let's find out about them.

Steiner systems

If n is a positive integer, we use the expressions *n-set* and *n-subset* to mean an n-element set and an n-element subset. A *Steiner system* $S(p, q, r)$ is a collection S of q-subsets of an r-set R, such that every p-set in R is contained in exactly one of the q-sets in S. An $S(1, q, r)$ is just a partition of an r-set into q-sets, so that these exist if and only if r is a multiple of q. It is known that $S(2, 3, r)$s exist if and only if $r \equiv 1$ or 3 mod 6 and $S(3, 4, r)$s exist if and only if $r \equiv 2$ or 4 mod 6. Steiner systems $S(2, 3, r)$ are also block designs known as *Steiner triple systems*; here is $S(2, 3, 7)$, namely the (7, 3, 1) symmetric design with blocks A, B, C, D, E, F, and G:

$$A = 124, \quad B = 235, \quad C = 346, \quad D = 450, \quad E = 561, \quad F = 602, \quad G = 013. \quad (5)$$

(You can construct an $S(3, 4, 8)$ from the $S(2, 3, 7)$: adjoin ∞ to each of the blocks of the $S(2, 3, 7)$, and include the complement in $\{0, 1, 2, 3, 4, 5, 6\}$ of each block in the $S(2, 3, 7)$.)

For $p \geq 4$, the story is different: very few of these are known, and one reason is that there are restrictions on the parameters p, q, and r, namely:

THEOREM 5. *If S is an $S(p, q, r)$ defined on the r-set R, then S contains $\binom{r}{p}/\binom{q}{p}$ q-sets, and for $0 \leq j < p$:*

(a) $\binom{r-j}{p-j}/\binom{q-j}{p-j}$ *is an integer;*

(b) *every j-subset of R belongs to exactly $\binom{r-j}{p-j}/\binom{q-j}{p-j}$ q-sets of S;*

(c) *there exists an $S(p-j, q-j, r-j)$ on an $(r-j)$-subset of R.*

Proof. Each of the $\binom{r}{p}$ p-sets in R belongs to a unique q-set in S and each such q-set contains $\binom{q}{p}$ p-sets; hence, S contains $\binom{r}{p}/\binom{q}{p}$ q-sets. It follows that $\binom{r}{p}/\binom{q}{p}$ is an integer, which establishes (a) for $j = 0$. Now fix $x \in R$. Let $S_x = \{Y | Y \text{ is a } q\text{-set in } R \text{ containing } x\}$. Since each p-set containing x belongs to a unique q-set $Y \in S_x$, it follows that $S'_x = \{Y - \{x\} | Y \in S_x\}$ is a collection of $(q-1)$-subsets of $R - \{x\}$, such that each $(p-1)$-subset of $R - \{x\}$ belongs to a unique $(q-1)$-set in S'_x. In short, S'_x is an $S(p-1, q-1, r-1)$ on the set $R - \{x\}$; by the above, it follows that S_x contains exactly $\binom{r-1}{p-1}/\binom{q-1}{p-1}$ q-sets of S. This establishes (b) and (c) for $j = 1$. Continuing inductively, we see that if an $S(p, q, r)$ exists, then so does an $S(p-j, q-j, r-j)$ for $0 \leq j \leq p-1$; from this, we may deduce (b) and (c) for $0 \leq j < p$. ∎

The $S(p-j, q-j, r-j)$ systems obtained in this way from an $S(p, q, r)$ are said to be *derived* from the $S(p, q, r)$. Every known Steiner system $S(4, q, r)$ is derived from an $S(5, q+1, r+1)$, and very few Steiner systems with $p \geq 4$ are known at all. It turns out that we can use the $(11, 5, 2)$ biplane and the binary Golay codes to construct two pairs of these rare Steiner systems, namely $\{S(4, 5, 11), S(5, 6, 12)\}$ and $\{S(4, 7, 23), S(5, 8, 24)\}$.

We now construct $S(5, 6, 12)$ and the systems derived from it—in particular, $S(4, 5, 11)$—by means of a unified approach, beginning with the $(11, 5, 2)$ biplane. Let $B_1 = \{1, 3, 4, 5, 9\}$, the first block in the $(11, 5, 2)$ biplane, and let $B := B_1 \cup \{\infty\}$. Denote the set $\{0, 1, \ldots, 10\}$ by $[0\,..\,10]$. In what follows, addition and subtraction are all mod 11, except that $\infty \pm x = \infty$ for all x. If Y is a set of numbers and m is a number, then we define $Y + m := \{y + m | y \in Y\}$. For example, $B + 6 = \{1+6, 3+6, 4+6, 5+6, 9+6, \infty+6\} = \{7, 9, 10, 0, 4, \infty\}$.

Define the mappings s and σ to be permutations on $[0\,..\,10]$ and $[0\,..\,10] \cup \{\infty\}$, respectively, by

$$\sigma = (1\ 10)(2\ 5)(3\ 7)(4\ 8)(6\ 9) \quad \text{and} \quad s = (0\ \infty) \circ \sigma.$$

Now, if f is a permutation and Y is a set, then define $f(Y)$ to be $\{f(y) : y \in Y\}$. For example, since $B + 6 = \{7, 9, 10, 0, 4, \infty\}$, we see that

$$\begin{aligned} s(B+6) &= s(\{7, 9, 10, 0, 4, \infty\}) = \{s(7), s(9), s(10), s(0), s(4), s(\infty)\} \\ &= \{3, 6, 1, \infty, 8, 0\}, \quad \text{and so} \\ s(B+6) + 3 &= \{6, 9, 4, \infty, 0, 3\}. \end{aligned}$$

We now construct the Steiner systems as follows:

$$S(5, 6, 12) = \{B + k | k \in [0\,..\,10]\} \cup \{s(B + k) + j \,|\, j, k \in [0\,..\,10]\};$$

$$S(4, 5, 11) = \{B_1 + k | k \in [0\,..\,10]\} \cup \{\sigma(B_1 - n) + k : n \in B_1, k \in [0\,..\,10]\};$$

$S(3, 4, 10) =$ blocks of $S(4, 5, 11)$ containing 10, with 10 deleted; and

$S(2, 3, \ 9) =$ blocks of $S(3, 4, 10)$ containing 0, with 0 deleted.

A table on page 100 lists the blocks for $S(4, 5, 11)$ and the list for $S(5, 6, 12)$ is available at the MAGAZINE web site; don't peek until you've tried your hand at constructing them yourself. Notice that the blocks of the $(11, 5, 2)$ biplane appear in $S(4, 5, 11)$ as its first column.

There are many ways to construct $S(5, 8, 24)$ (as, indeed, there are to construct $S(5, 6, 12)$), and one way is to use the Golay code G_{24}. By Theorem 5, if $S(5, 8, 24)$ exists, then it contains $\binom{24}{5}/\binom{8}{5} = 759$ 8-sets. This just happens to be the exact number of codewords of Hamming weight 8 in G_{24}. For example, all rows but the last in the generating matrix $\mathbf{A}$ (see Equation (4)) are codewords of weight 8. Let us number the columns of $\mathbf{A}$ with the customary numbering scheme $1, 2, \ldots, 22, 0, \infty$. If $c = c_1 c_2 \cdots c_\infty$ is a weight-8 codeword, then $O_c = \{i | c_i = 1\}$ is an 8-subset of $\{1, 2, \ldots, 22, 0, \infty\}$. The system $S(5, 8, 24)$ consists of these 759 so-called *octads*, and we construct the derived systems as follows:

$$S(5, 8, 24) = \text{codewords of weight 8 in } G_{24};$$

$$S(4, 7, 23) = \text{octads of } S(5, 8, 24) \text{ containing } \infty, \text{ with } \infty \text{ deleted};$$

$$S(3, 6, 22) = \text{blocks of } S(4, 7, 23) \text{ containing 0, with 0 deleted; and}$$

$$S(2, 5, 21) = \text{blocks of } S(3, 6, 22) \text{ containing 22, with 22 deleted.}$$

$S(5, 8, 24)$ has many remarkable properties and connections, and we have obviously left out many details. To do justice to this truly amazing object requires quite a journey. Thompson's book [**12**] is an excellent starting point; it certainly was for me.

One of the notable aspects of $S(5, 8, 24)$ is something it shares with the other Steiner systems, namely, a high degree of symmetry. Studying this symmetry leads us to the connection between the $(11, 5, 2)$ biplane and the Mathieu groups.

Automorphisms, transitivity, simplicity, and the Mathieu groups

An *automorphism* of a Steiner system S is a permutation of the underlying r-set that also permutes the q-sets of S among themselves. For example, the permutation $a = (2\ 4)(5\ 6)$ on the set $\{0, 1, 2, 3, 4, 5, 6\}$ is an automorphism of $S(2, 3, 7)$ (see Equation (5)). Using the labeling convention from that equation, you can check that a switches B and C, switches D and F, and leaves A, E, and G fixed. That is, viewed as a permutation on $S(2, 3, 7)$, $a = (B\ \ C)(D\ \ F)$.

You may recall that the automorphisms of the $(11, 5, 2)$ biplane form a group under composition, and the same is true for the automorphisms of a Steiner system. As before, we write $Aut(S)$ for the automorphism group of the Steiner system S. In general, Steiner systems have a large number of automorphisms. For example, $S(2, 3, 7)$ consists of seven triples, and yet $Aut(S(2, 3, 7))$ is isomorphic to $PSL(2, 7)$, the group of order 168 generated by the permutations $a = (2\ 4)(5\ 6)$ and $b = (0\ 1\ 2\ 3\ 4\ 5\ 6)$ on the set $\{0, 1, 2, 3, 4, 5, 6\}$. For example, you can show that, as a permutation on $S(2, 3, 7)$, $ab^2 = (A\ \ B\ \ F)(C\ \ E\ \ G)$.

The automorphism groups of $S(4, 5, 11)$, $S(5, 6, 12)$, $S(4, 7, 23)$, and $S(5, 8, 24)$ are known as the Mathieu groups M_{11}, M_{12}, M_{23}, and M_{24}, respectively. First, we'll learn about their origin and why they are important, and then we'll describe them.

Émile Mathieu (1835–1890) first constructed the groups bearing his name in two papers summarizing work from his doctoral thesis. The Mathieu groups are special in two ways: first, they are *multiply transitive*, and second, they are *simple*—the first of the so-called *sporadic* finite simple groups ever described. Let us see what these terms mean.

A group of permutations G on a set A is called *k-transitive* if for every pair of ordered k-tuples $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_k)$ of elements of A, there exists $g \in G$ such that $g(a_i) = b_i$ for $1 \leq i \leq k$. We call G *transitive* (respectively, *multiply transitive*) if it is 1-transitive (respectively, k-transitive for some $k > 1$). A k-transitive group is also $(k-1)$-transitive. For example, the alternating group $A_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ is transitive, but not multiply transitive. The group $PSL(2, 7)$ is 2-transitive, but not 3-transitive. The symmetric group S_n, consisting of all permutations on $\{1, 2, \ldots, n\}$, is n-transitive. Now, one special feature of the Mathieu groups is that they are highly transitive. Theorem 6 tells the story; you can find a proof in many texts about finite group theory [**3, 11**].

THEOREM 6.

(a) *If G is* 4*-transitive, then G is isomorphic to* (i) *a symmetric group S_n for some $n \geq 4$,* (ii) *an alternating group A_n for some $n \geq 6$, or* (iii) *M_n for $n = 11, 12, 23$, or* 24.

(b) *If G is* 5*-transitive, then G is isomorphic to* (i) *a symmetric group S_n for some $n \geq 5$,* (ii) *an alternating group A_n for some $n \geq 7$,* (iii) *M_{23}, or* (iv) *M_{24}.*

The Mathieu groups are also *simple*, and to understand what that means, we need to recall an idea from matrix algebra: Two matrices A and B are *similar* if there exists an invertible matrix Q such that $B = Q^{-1}AQ$. We can carry this idea over into groups: two group elements a and b are *conjugate* if there exists a group element g such that $b = g^{-1}ag$. (Remember, all elements of a group are invertible.) For example, if $a = (1\ 2)$, $b = (1\ 3)$, and $g = (1\ 2\ 3)$, then you can show that $b = g^{-1}ag$.

A special property of some subgroups is that of normality: A subgroup H of a group G is *normal* if for all $h \in H$ and for all $g \in G$, H contains $g^{-1}hg$. For example, let $S = \{(1), (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$, the group of all permutations of $\{1, 2, 3\}$; let $A = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ and $C = \{(1), (1\ 2)\}$. You can check that A and C are both subgroups of S, that A is normal, and that C is not normal. If G is an abelian (commutative) group, then all subgroups are normal—for, if $h \in H$ and $g \in G$, then $g^{-1}hg = g^{-1}gh = h \in H$ by commutativity.

A group containing no normal subgroups except itself and the identity subgroup is called *simple*. Just as prime numbers are the (multiplicative) building blocks by which we construct all the integers, so simple groups are the building blocks for constructing all finite groups. A major achievement of twentieth-century mathematics, featuring such luminaries as Chevalley, Feit, Thompson, Conway, Fischer, Gorenstein, and many others, was the complete classification of finite simple groups. The upshot of this effort, spanning some 15,000 journal pages (!), is that all finite simple groups belong to a few well-studied infinite families—except for twenty-six so-called *sporadic* groups. And the Mathieu groups were the very first sporadic groups ever described. Speaking of which:

There are many ways to describe the Mathieu groups; here is one: Let s, t, and u be the permutations defined by

$$s = (0\ \infty)(1\ 10)(2\ 5)(3\ 7)(4\ 8)(6\ 9),$$

$$t = (0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10), \quad \text{and}$$

$$u = (3\ 9\ 4\ 5)(2\ 6\ 10\ 7).$$

Then M_{11} is the group generated by t and u, and M_{12} is the group generated by s, t, and u. And yes, *s is* the same permutation that we used to construct $S(5, 6, 12)$.

Let α, β, and γ be the permutations defined on $\{0, 1, \ldots, 22, \infty\}$ by

$$\alpha = (2\ 16\ 9\ 6\ 8)(4\ 3\ 12\ 13\ 18)(10\ 11\ 22\ 7\ 17)(20\ 15\ 14\ 19\ 21),$$

$$\beta = (0\ 1\ \ldots\ 21\ 22), \quad \text{and}$$

$$\gamma = (0\ \infty)(1\ 22)(2\ 11)(3\ 15)(4\ 17)(5\ 9)(6\ 19)(7\ 13)(8\ 20)(10\ 16)(12\ 21)(14\ 18).$$

Then M_{23} is the group generated by α and β, and M_{24} is the group generated by α, β, and γ. See Thompson [**12**] for more details.

We can now see how M_{11} and M_{12} go together in a pair, and the same is true of M_{23} and M_{24}; to cement their connection with the (11, 5, 2) biplane further, it turns out that the number of elements in each of these groups is divisible by 11.

With that, our whirlwind tour of the (11, 5, 2) biplane, its symmetries, and its connections with six pairs of combinatorial gems is done. Quite a tale!

Questions

- *Where can I go to learn more about these things?* Look in the bibliography. Beth, Jungnickel, and Lenz [**1**] will take you a long way into the world of combinatorial designs, including all the ones mentioned in this paper and many more. Hughes and Piper [**6**] will do the same; they pay special attention to biplanes, and the previously mentioned unlabeled version of FIGURE 2 appears on the cover of their book. Marshall Hall [**5**] has a great deal of information on difference sets. A recent article in this MAGAZINE [**2**] will tell you more about difference sets and squares mod p. MacWilliams and Sloane [**8**] and Pless [**9**] are two standard works on error-correcting codes. Carmichael [**3**] has a whole lot of information about the Mathieu groups, although his presentation is a bit old-fashioned; for a more modern treatment, Rotman [**11**] is one of the best. Finally, Thompson [**12**] has all of these in a wonderfully written book. Happy Reading!
- *You said that* $Aut((11, 5, 2))$ *is isomorphic to* $PSL(2, 11)$. *How do you prove that?* It turns out that both $PSL(2, 11)$ and $Aut((11, 5, 2))$ are generated by two elements c and d, for which $c^2 = d^3 = (cd)^{11} = ((cd)^3(cd^2)^3)^2 = 1$, the identity permutation. Two automorphisms of (11, 5, 2) that fill the bill are $c = (1\ 3)(2\ 5)(4\ X)(7\ 9)$ and $d = (3\ 4\ 5)(2\ 6\ 0)(7\ 8\ X)$. Try it and see.
- *Any other tidbits about* $G = Aut((11, 5, 2))$*?* Here are a few. (1) It so happens that the group $H = Stab_G(B_1)$ has order 60 and is isomorphic to A_5, the alternating group on 5 elements. A picture of the (11, 5, 2) biplane that would show this would indeed be spectacular. (2) Constructing one to depict the automorphism d (of order 3) from the previous bullet is a good warm-up for (1). (3) G contains an automorphism of order 6: find one and draw the associated picture. (4) Recall that $|G| = 660$, which is divisible by 4; does G contain an automorphism of order 4?
- *You told us about four Mathieu groups, but I read somewhere that there are five of them. What is the fifth Mathieu group, and why did you leave it out?* Right you are; it's called M_{22}. This group is a permutation group on a 22-element set that is simple and triply transitive. One way to describe M_{22} is that it is the set of all permutations

in M_{23} that leave 0 fixed. It is a subgroup of index two of the group of automorphisms of $S(3, 6, 22)$. (The additive group of even integers is a subgroup of index two of the integers.) I left it out because it is not part of a pair.

- *Are there any interesting problems associated with the* $(11, 5, 2)$ *biplane, or with biplanes in general?* Several come to mind. Recall that a biplane is a symmetric (v, k, λ) design with $\lambda = 2$. (1) There are biplanes with $v < 11$; find them, find their automorphism groups, and draw some pictures. (2) Two block designs are *isomorphic* if there exists a one-to-one correspondence between the underlying sets of varieties that induces such a correspondence between the sets of blocks. Show that every $(11, 5, 2)$ biplane is isomorphic to the one presented in this paper. (3) Construct a $(16, 6, 2)$ biplane. Then, construct another one not isomorphic to the first one. How do you show that two designs are not isomorphic? Interesting question! (4) One problem is particularly intriguing. Recall that a finite projective plane is a symmetric design with $\lambda = 1$. It turns out that if q is a prime power, then there exists a finite projective plane with parameters $(q^2 + q + 1, q + 1, 1)$; as a consequence, there are infinitely many finite projective planes. So we may ask the question, "Are there infinitely many biplanes?" Nobody knows! Other than the ones alluded to in (1), the only known biplanes are for $k = 5$, 6, 9, 11, and 13. Are there others? Find the answer and become famous.

REFERENCES

1. T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, 2nd ed., Cambridge University Press, New York, 1999.
2. Ezra Brown, The many names of (7, 3, 1), this MAGAZINE **75** (2002), 83–94.
3. Robert D. Carmichael, *Introduction to the Theory of Groups of Finite Order*, Dover Publications, New York, 1956.
4. Richard K. Guy, The unity of combinatorics, in *Combinatorics Advances*, C. J. Colburn and E. S. Mahmoodian (eds.), Kluwer, 1995, 129–159.
5. Marshall Hall, Jr., *Combinatorial Theory*, 9th ed., Blaisdell Publishing Company, Waltham, MA, 1967.
6. D. R. Hughes and F. C. Piper, *Design Theory*, Cambridge University Press, New York, 1985.
7. T. A. Kirkman, On a problem in combinations, *Camb. Dublin Math. J.* **2** (1847), 191–204.
8. F. Jessie MacWilliams and Neil J. A. Sloane, *The Theory of Error-Correcting Codes*, 2nd reprint, North-Holland Mathematical Library **16**, North-Holland, New York, 1983.
9. Vera Pless, *Introduction to the Theory of Error-Correcting Codes*, 2nd ed., Wiley, New York, 1989.
10. George Pólya, *How To Solve It*, 2nd ed., Doubleday, Garden City, NY, 1957.
11. Joseph J. Rotman, *An Introduction to the Theory of Groups*, 4th ed., Springer-Verlag, New York, 1995.
12. Thomas M. Thompson, *From Error-Correcting Codes Through Sphere Packings to Simple Groups*, Carus Mathematical Monograph No. 21, Mathematical Association of America, Washington, DC, 1983.
13. W. S. B. Woolhouse, Prize question 1733, *Lady's and Gentleman's Diary*, 1844.

13459	07293	03618	0412*X*	06*X*59	05784
2456X	183*X*4	14729	15230	1706*X*	16895
35670	29405	2583*X*	26341	28170	279*X*6
46781	3*X*516	36940	37452	39281	38*X*07
57892	40627	47*X*51	48563	4*X*392	49018
689X3	51738	58062	59674	504*X*3	5*X*129
79X04	62849	69173	6*X*785	61503	6023*X*
8X015	7395*X*	7*X*284	70896	72615	71340
90126	84*X*60	80395	819*X*7	83726	82451
X1237	95071	914*X*6	92*X*08	94837	93562
02348	*X*6182	*X*2507	*X*3019	*X*5948	*X*4673

The Steiner system S(4, 5, 11) and the (**11**, **5**, **2**) **design** from Brown's article on page 87