ARTICLES

Kirkman's Schoolgirls Wearing Hats and Walking through Fields of Numbers

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

KEITH E. MELLINGER
University of Mary Washington
Fredericksburg, VA 22401
kmelling@umw.edu

Fifteen young ladies at school

Imagine fifteen young ladies at the Emmy Noether Boarding School—Anita, Barb, Carol, Doris, Ellen, Fran, Gail, Helen, Ivy, Julia, Kali, Lori, Mary, Noel, and Olive. Every day, they walk to school in the Official ENBS Formation, namely, in five rows of three each. One of the ENBS rules is that during the walk, a student may only talk with the other students in her row of three. These fifteen are all good friends and like to talk with each other—and they are all mathematically inclined. One day Julia says, "I wonder if it's possible for us to walk to school in the Official Formation in such a way that we all have a chance to talk with each other at least once a week?" "But that means nobody walks with anybody else in a line more than once a week," observes Anita. "I'll bet we can do that," concludes Lori. "Let's get to work." And what they came up with is the schedule in TABLE 1.

TABLE 1: Walking to school

MON	TUE	WED	THU	FRI	SAT	SUN
a, b, e	a, c, f	a, d, h	a, g, k	a, j, m	a, n, o	a, i, l
c, l, o	b, m, o	b, c, g	b, h, l	b, f, k	b, d, i	b, j, n
d, f, m	d, g, n	e, j, o	c, d, j	c, i, n	c, e, k	c, h, m
g, i, j	e, h, i	f, l, n	e, m, n	d, e, l	f, h, j	d, k, o
h, k, n	j, k, l	i, k, m	f, i, o	g, h, o	g, l, m	e, f, g

TABLE 1 was probably what T. P. Kirkman had in mind when he posed the Fifteen Schoolgirls question in 1850. Appearing in the unlikely-sounding *Lady's and Gentlemen's Diary* [**15**], it reads as follows:

> Fifteen young ladies of a school walk out three abreast for seven days in succession: it is required to arrange them daily so that no two shall walk abreast more than once.

Kirkman's publication of this problem and solution [**15, 16**] is one of the starting points for what has become the vast modern field of combinatorial design theory. Its

poser, Thomas Pennyngton Kirkman (1806–1895), is one of the more intriguing figures in the history of mathematics. He published his first mathematical paper when he was 40, and was the first to describe many structures in discrete mathematics. Among these are block designs, which form the basis for the statistical design of experiments; bipartite graphs, which are essential for such problems as classroom scheduling and medical school admissions; and Hamiltonian circuits, which are at the heart of the famous Traveling Salesman Problem. (Biggs [**2**] gives more details about Kirkman's life and work.) For these achievements, combinatorialists regard him as the "Father of Design Theory"—yet his fame outside the field rests entirely on the Schoolgirls Problem and his solution.

This story is about the very problem that made Kirkman famous. His solution is an example of a *resolvable* $(15, 35, 7, 3, 1)$-*design*, and we begin by explaining what those words and numbers mean. We describe how one of us found such a design by looking in a most unlikely place: the algebraic number field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$. This proves to be a particularly fertile field in which several other block designs grow. We talk about spreads and packings in finite geometries, how a particular packing in the geometry $PG(3, 2)$ answers Kirkman's question, and how the $PG(3, 2)$ design is really the same as the number field design. Finally, we show how our design is a solution to a certain problem in recreational mathematics called the Fifteen Hats Problem.

We begin by talking about block designs.

Block designs and Kirkman Triple Systems

Design theory began with Euler's studies of Latin squares in the 18th century, interest in which was recently rekindled with the world-wide popularity of Sudoku. Many decades after their invention by Kirkman, block designs appeared in connection with R. A. Fisher's work [**10, 11**] on the statistical design of agricultural experiments, and the first comprehensive mathematical study of the field was due to R. C. Bose [**4**]. More recently, they have found applications in coding theory, cryptography, network design, scheduling, communication theory, and computer science. Finally, designs have always appealed to mathematicians because of their elegance, beauty, high degree of symmetry, and connections with many other fields of mathematics [**5**].

A *balanced incomplete block design* with parameters v, b, r, k, and λ is a collection $\mathcal{B}$ of b subsets (or *blocks*) of a v-element set V of objects (or *varieties*) such that each block contains k varieties, each variety appears in r blocks and each pair of distinct varieties appears together in λ blocks. Such a design is also called a (v, b, r, k, λ)-design. We say a design like this is *incomplete* if $k < v$. From a combinatorial point of view, complete designs are not very interesting. However, statisticians do use them to design experiments.

The five parameters in these designs are not independent. Since there are b blocks, each of size k, there are bk occurrences of varieties in the design. On the other hand, there are v varieties, each occurring in r blocks, and so a total of vr varieties appear in the design. Hence $bk = vr$. A similar counting argument shows that $r(k-1) = \lambda(v-1)$. Hence

$$r = \frac{\lambda(v-1)}{k-1} \quad \text{and} \quad b = \frac{\lambda v(v-1)}{k(k-1)}.$$

Because of these relations, such a design is frequently called a (v, k, λ)-design. (There are more details about block designs in [**5**].)

Given a block design with varieties $x_1, \ldots, x_v$ and blocks $B_1, \ldots, B_b$, an efficient way to represent it is by its *incidence matrix*. This is a $b \times v$ matrix $M = [m_{ij}]$, where $m_{ij} = 1$ if $x_j \in B_i$ and $m_{ij} = 0$ otherwise.

A reading of the Kirkman Schoolgirls Problem reveals that he first asks for an arrangement of 15 schoolgirls into sets of size three such that each pair of girls is present in at most one of these triples. There are five triples for each of seven days, making 35 triples in all. Moreover, each girl appears in just one triple each day, and over seven days, each girl would thus appear with each other girl exactly once. We conclude that Kirkman is asking for a way to arrange the girls into a $(15, 3, 1)$-design. (The incidence matrix for Kirkman's design will reappear when we ask the schoolgirls to wear hats.)

But there is more: he asks for a way to arrange the $b = 35$ triples into seven days of five triples each, so that each girl appears in exactly one triple each day. Such a design, whose b blocks can be arranged into r *parallel* classes of $n = v/k$ blocks each such that each variety appears exactly once in each class, is called *resolvable*. For such a design to exist, v must be a multiple of k. In Kirkman's honor, a resolvable $(3n, 3, 1)$-design is called a *Kirkman Triple System*. (A $(v, 3, 1)$-design is called a *Steiner Triple System*, despite the fact that Kirkman described them six years before Jakob Steiner's publication on the subject—but that's another story.)

Do Kirkman Triple Systems exist? Yes, they do. The smallest possibility has $v = 3$, with exactly one block and one parallel class, but the smallest nontrivial case has $v = 9$. Construction begins with the magic square of order 3, that familiar arrangement of the numbers 1 through 9 into a 3×3 grid such that the triples of numbers in each row, each column and on the two main diagonals add up to 15. The three rows, three columns, three extended diagonals parallel to the principal diagonal, and three more parallel to the principal contrary diagonal form the four parallel classes of a resolvable $(9, 3, 1)$-design. The following picture tells the tale, with the magic square on the left and the four parallel classes of the resolvable $(9, 3, 1)$-design on the right:

8	1	6
3	5	7
4	9	2

{1, 6, 8}	{3, 5, 7}	{2, 4, 9}
{1, 5, 9}	{2, 6, 7}	{3, 4, 8}
{1, 4, 7}	{2, 5, 8}	{3, 6, 9}
{1, 2, 3}	{4, 5, 6}	{7, 8, 9}

The next smallest case has $v = 15$, which is the design Kirkman sought in his query; where do we look? If we could find a structure containing fifteen objects arranged in thirty-five sets, with three objects per set, that would be a place to start. It happens that there are such structures, and we find one of them in the world of algebraic number theory—specifically, in the number field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$. The field K contains several interesting designs, and we'll talk about them, but first we supply some background about this area of mathematics.

$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$ and the designs it contains

Évariste Galois (1811–1832) described relations involving the roots of polynomials, number fields, and finite groups, now known as Galois theory. One basic idea is that if $p(x)$ is a polynomial with rational coefficients, then there is a smallest subfield of the complex numbers $\mathbb{C}$ containing all the roots of $p(x)$. This is the *splitting field* of p over $\mathbb{Q}$. If $a, b, \ldots \in \mathbb{C}$, we write $\mathbb{Q}(a, b, \ldots)$ to mean the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and $a, b, \ldots$. For example, the splitting field of the polynomial $p(x) =$

$(x^2-2)(x^2-3)(x^2-5)$ is the field $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$. Now it is a fact that $\mathbb{Q}(a,b,\dots)$ is a vector space over $\mathbb{Q}$, and the *degree* of $\mathbb{Q}(a,b,\dots)$ over $\mathbb{Q}$ is the dimension of this vector space. These splitting fields have a good bit of internal structure, which we illustrate with the field $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$, described in [**5**].

Now by definition, the *biquadratic* (degree-4) field $\mathbb{Q}(\sqrt{2},\sqrt{3})$ contains the two elements $\sqrt{2}$ and $\sqrt{3}$, and since it is a field, it also contains $\sqrt{2}\sqrt{3}=\sqrt{6}$. Hence $\mathbb{Q}(\sqrt{2},\sqrt{3})$ also contains three *quadratic* (degree-2) subfields: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{6})$. A similar argument shows that $\mathbb{Q}(\sqrt{6},\sqrt{10})$ contains $\sqrt{15}=\sqrt{6}\sqrt{10}/2$, and so it also contains the three quadratic subfields $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{10})$, and $\mathbb{Q}(\sqrt{15})$. In the same vein, one can show that $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ contains seven quadratic subfields $\mathbb{Q}(\sqrt{d})$, for $d=2$, 3, 5, 6, 10, 15, and 30, and seven *biquadratic* subfields $\mathbb{Q}(\sqrt{d_1},\sqrt{d_2})$. Not only does each biquadratic subfield contain three quadratic subfields, but each quadratic is contained in three biquadratics, and in [**5**], these subfields of $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ are shown to form a $(7,7,3,3,1)$-design with the biquadratic fields as the blocks and the quadratic fields as the varieties. Such a design, in which $b=v$ and $r=k$, is called a *symmetric* design, and we will encounter some more symmetric designs later in this section.

We now turn to the polynomial $p(x)=(x^2-2)(x^2-3)(x^2-5)(x^2-7)$, whose splitting field is the degree-16 field $K=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{7})$, the smallest subfield of the complex numbers containing $\mathbb{Q}(\sqrt{d})$ for $d=2$, 3, 5, and 7. Now let $S=\{2,3,5,6,7,10,14,15,21,30,35,42,70,105,210\}$. Then K contains the 15 quadratic subfields $\mathbb{Q}(\sqrt{d})$ for $d\in S$. Moreover, each pair of these quadratics is contained in a unique biquadratic subfield of K, and each biquadratic contains three quadratics. A counting argument shows that K contains 35 biquadratic subfields $\mathbb{Q}(\sqrt{d_1},\sqrt{d_2})$, and it is straightforward to show that each quadratic is contained in seven biquadratics.

Now consider the block design with the 15 quadratic subfields of K as varieties and the 35 biquadratic subfields of K as blocks. Our work in the previous paragraph shows that these form a block design with $v=15$, $b=35$, $r=7$, $k=3$, and $\lambda=1$, that is, a (15, 3, 1)-design, which we call KS for short. But is KS resolvable?

In fact, it is, and TABLE 2 shows the seven columns that are the seven parallel classes. The three numbers in each of the 35 cells in this table determine a block, that is, one of the 35 biquadratic subfields of K. We began by placing the seven biquadratic subfields containing $\mathbb{Q}(\sqrt{2})$ in separate classes across the top row and proceeded, mainly by trial and error, to arrange the thirty-five blocks in seven parallel classes. The end result is a resolvable (15, 3, 1)-design—in short, a solution to Kirkman's Schoolgirls problem.

But that is not all. The field K also contains another resolvable (15, 3, 1) design as well as two other types of designs. We construct the other Kirkman design as follows.

TABLE 2: The Kirkman design in $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{7})$

MON	TUE	WED	THU	FRI	SAT	SUN
2, 3, 6	2, 5, 10	2, 7, 14	2, 15, 30	2, 21, 42	2, 35, 70	2, 105, 210
5, 21, 105	3, 70, 210	3, 5, 15	3, 14, 42	3, 35, 105	3, 7, 21	3, 10, 30
7, 30, 210	6, 14, 21	6, 35, 210	5, 7, 35	5, 6, 30	5, 42, 210	5, 14, 70
10, 14, 35	7, 15, 105	10, 42, 105	6, 70, 105	7, 10, 70	6, 10, 15	6, 7, 42
15, 42, 70	30, 35, 42	21, 30, 70	10, 21, 210	14, 15, 210	14, 30, 105	15, 21, 35

The blocks are the 35 biquadratic subfields of K, and the varieties are the 15 *octic* (degree-8) subfields of K, which we number a through o as in TABLE 3. Notice that a is the subfield $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, with which we began this section. But in a reversal of the previous construction, a variety (octic field) is a member of those blocks (biquadratic fields) *that it contains as a subfield*. That is, "contains" means "is a subfield of" in this context. Thus, the "block" $\mathbb{Q}(\sqrt{21}, \sqrt{35})$ "contains" the three "varieties" d, o and k, as shown in TABLE 3.

It is straightforward to show that each of the 35 biquadratic subfields of K is a subfield of exactly three of these octic fields, each octic contains seven biquadratic subfields, and each pair of biquadratics are subfields of a unique octic. Thus, we have another (15, 3, 1) -design, which we call KS^*.

Is KS^* resolvable? Yes, it is, and to see this, we look at TABLE 2 again. In it, each biquadratic is designated by the triple of *quadratics it contains*. If we replace each biquadratic in TABLE 2 by the triple of *octics that contain it*, we are led to TABLE 1, the arrangement found by the fifteen ladies at the ENBS.

The field K contains fifteen octic subfields, and each of these contains seven quadratic subfields. It turns out that each quadratic appears in seven octics, and that each pair of quadratics appear together in exactly three octics. This gives us a symmetric (15, 7, 3)-design OQ with the quadratics as varieties and the octics as blocks. Each row of TABLE 3 begins with a letter referring to an octic field, followed by seven numbers $d_1, \ldots, d_7$; these are the values of d for which $Q(\sqrt{d})$ is contained in that octic field. For example, line l refers to the octic field $L = \mathbb{Q}(\sqrt{3}, \sqrt{10}, \sqrt{14})$. It contains the seven quadratic subfields $\mathbb{Q}(\sqrt{r})$ for $r = 3$, 10, 14, 30, 35, 42, and 105.

Now, the elements of the blocks in TABLE 3 can themselves be arranged into block designs. For each of the 15 octic subfields of K contains 7 biquadratic subfields (the

TABLE 3: The (15, 7, 3)-design OQ in $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$

Octic Field	**Contains $\mathbb{Q}(\sqrt{d})$ for these d**
a	2, 3, 5, 6, 10, 15, 30
b	2, 3, 7, 6, 14, 21, 42
c	2, 5, 7, 10, 14, 35, 70
d	3, 5, 7, 15, 21, 35, 105
e	2, 3, 6, 35, 70, 105, 210
f	2, 5, 10, 21, 42, 105, 210
g	2, 7, 14, 15, 30, 105, 210
h	3, 5, 14, 15, 42, 70, 210
i	3, 7, 10, 21, 30, 70, 210
j	5, 6, 7, 30, 35, 42, 210
k	2, 15, 21, 30, 35, 42, 70
l	3, 10, 14, 30, 35, 42, 105
m	5, 6, 14, 21, 30, 70, 105
n	6, 7, 10, 15, 42, 70, 105
o	6, 10, 14, 15, 21, 35, 210

blocks) as well as 7 quadratic subfields (the varieties). Each biquadratic contains 3 quadratics, each quadratic is contained in 3 biquadratics, and each pair of quadratics lie in a unique biquadratic. Thus, each block is a triple of quadratics, and we conclude that K contains fifteen symmetric $(7, 3, 1)$-designs. Continuing with line l, we list the triples of the $(7, 3, 1)$-design contained in the octic field L here:

$$10, 14, 35;\ 30, 35, 42;\ 10, 42, 105;\ 3, 14, 42;\ 3, 35, 105;\ 14, 30, 105;\ 3, 10, 30$$

As an exercise, find these seven triples in TABLE 2, and observe that they occur in different columns.

Finally, if D is a symmetric design, then the *dual* design D^* of D is obtained from D by a formal exchange of blocks and varieties. Thus, if the variety x belongs to the block B in D, then the variety B belongs to the block x in D^*. In this way, we obtain the dual OQ^* of the $(15, 7, 3)$ symmetric design OQ depicted in TABLE 3, again by a formal exchange of blocks and designs. We note that this construction fails for nonsymmetric designs, that is designs in which $v \neq b$.

Exchanging the roles of blocks and varieties in a block design is analogous to exchanging the roles of points and lines in projective geometry. To see this more clearly, we need to pass to a geometric description of KS. So, let's talk about finite projective geometries and spreads.

Spreads in $PG(3, 2)$ and the geometry of Kirkman

One very elegant way to generate a solution to the Kirkman Schoolgirls problem involves a nice partitioning and packing problem in finite projective geometry. Hundreds of years ago, projective spaces arose as extensions of the familiar real Euclidean spaces. The essential difference between Euclidean and projective spaces is that in projective spaces every pair of lines in a plane must intersect—there is no notion of parallelism. This lack of parallelism provides a nice duality to projective planes: Every two distinct points determine a unique line and every two distinct lines meet in a unique point. Lines can be skew, but this requires them to be noncoplanar. We will see examples of skew lines shortly since we will be mostly interested in finite projective 3-space, a place where lines can indeed be skew. But first let's talk more about finite projective geometry.

Just as with Euclidean geometry, there is a way to assign coordinates to the points of a finite projective space. We do this using a finite field (rather than the more familiar fields $\mathbb{R}$ or $\mathbb{Q}$). The classic example of a finite field is the set of integers $\{0, 1, \ldots, p-1\}$, with all arithmetic performed modulo p. But it can be shown that finite fields exist of any size that is a power of a prime. Typically, we use $q = p^k$ for a power of a prime and we let $GF(q)$ denote the finite field with q elements.

The technique for coordinatizing projective spaces is fairly easy and is a straightforward extension of the standard linear algebra techniques that we learn using real numbers. To construct a 3-dimensional projective space, we start with a 4-dimensional vector space over the finite field with q elements, $GF(q)$. The lattice of subspaces then gives us the geometry. That is, 1-dimensional subspaces represent points, 2-dimensional subspaces represent lines, and so on. This is the unique finite projective space of dimension 3 and *order* q, denoted by $PG(3, q)$. Notice that we have a representation problem for points: Since points are defined as 1-dimensional subspaces, all nonzero vectors in a particular 1-dimensional subspace represent the same projective point. This leads to the concept of *homogeneous coordinates* for projective spaces: When we use the nonzero vector (w, x, y, z) to represent a projective point, it is understood that any nonzero scalar multiple of this vector represents the same projective point. (The formalities involve equivalence classes of vectors.)

Now that we have a finite set and a nice representation, we can use standard counting techniques to determine some properties of our space. There are $q^4 - 1$ nonzero vectors in the entire vector space, and any *nonzero* scalar multiple of a nonzero vector gives the same projective point. Hence, the total number of points of $PG(3, q)$ is given by $(q^4 - 1)/(q - 1) = q^3 + q^2 + q + 1$. Similarly counting the number of 1-dimensional subspaces contained in a 2-dimensional subspace, we see that every line contains $q + 1$ points. Now consider the case when $q = 2$. Here the finite projective space $PG(3, 2)$ contains 15 points and every line contains 3 points. Sound familiar?

A solution to Kirkman's famous problem could be obtained with lines of $PG(3, 2)$. A solution would go something like this. First you would have to partition the projective space into lines. Such a partition of the points of $PG(3, q)$ into lines is called a *spread* by finite geometers. A spread in our setting would contain 5 disjoint lines (each containing 3 points). The points of our projective space would correspond to the girls, and the lines of our spread would correspond to the groups of girls walking together on the first day. To find the groups for the second day would require us to find a second spread such that no line from the first spread gets reused in the second spread. Then we continue in this fashion until we get 7 pairwise disjoint spreads (or 7 days' worth of partitions). Seems possible, I suppose. But are we satisfying the condition that no two girls walk together more than once? If this were not the case, then we would have two points of the projective space lying on two different lines. Recall that this violates the axiom for projective geometry requiring that every two distinct points determine a unique line. So, the geometric model actually guarantees us the desired property.

To solve Kirkman's problem, we would need 7 pairwise disjoint spreads (no two sharing a common line). Hence, we would need to use 35 different lines of the projective space. Do we have enough? Just as we counted points, we can easily count lines. Any two independent vectors would determine a 2-dimensional subspace. There are $q^4 - 1$ choices for a first vector and then $q^4 - q$ choices for a second vector that is independent from the first. Any particular 2-dimensional subspace will be counted by any pair of independent vectors in that subspace. Hence, the total number of 2-dimensional subspaces (that is, the number of lines of $PG(3, q)$) is

$$\frac{(q^4 - 1)(q^4 - q)}{(q^2 - 1)(q^2 - q)} = (q^2 + 1)(q^2 + q + 1).$$

Plugging in $q = 2$ gives us 35, precisely the number of lines we need.

Now, let's get back to the Kirkman solution in $PG(3, 2)$. In geometric terms, we are trying to partition the lines of $PG(3, 2)$ into 7 disjoint spreads. Such a partition of lines into spreads is known as a *packing*. It is fairly well-known that spreads and packings exist. Hirschfeld [**13**] gives details about how to actually construct such packings and even shows that they exist for projective 3-spaces of *any* order (that is, any value of q). The trick is to model $PG(3, q)$ not using a vector space, but rather using the finite field $GF(q^4)$. Then, subfields isomorphic to $GF(q^2)$ correspond to lines and some algebra can be used to show the existence of the spreads that we need. In general, the projective space $PG(3, q)$ contains $(q^2 + 1)(q^2 + q + 1)$ lines and a packing of $PG(3, q)$ is comprised of $q^2 + q + 1$ spreads, each of size $q^2 + 1$. Hence, packings of $PG(3, q)$ actually give a solution to a generalized Kirkman Schoolgirls problem:

> If $(q^2 + 1)(q + 1)$ schoolgirls go walking each day in $q^2 + 1$ rows of $q + 1$, they can walk for $q^2 + q + 1$ days so that each girl has walked in the same row as has every other girl and hence with no girl twice.

Incidentally, finite geometry provides a wealth of examples of designs, and Kirkman designs are no exception. By generalizing the spreads and packings described above,

one can construct resolvable $(3n, 3, 1)$ designs for many values of n simply by varying the dimension of the space you work in. A very thorough, albeit technical, description of these methods can be found in the book by Hirschfeld [**13**].

Let us represent the nonzero 4-bit strings (the projective points of $PG(3, 2)$) by the decimal integers they represent: $1 = 0001, 2 = 0010, \ldots, 10 = 1010, \ldots, 15 = 1111$. Then TABLE 4 shows a packing of the lines of $PG(3, 2)$ into 7 disjoint spreads, a solution to Kirkman's Schoolgirls Problem.

TABLE 4: The Kirkman design as a spread in $PG(3, 2)$

MON	TUE	WED	THU	FRI	SAT	SUN
1, 2, 3	1, 4, 5	2, 4, 6	1, 6, 7	3, 4, 7	3, 5, 6	2, 5, 7
4, 10, 14	2, 13, 15	1, 8, 9	2, 9, 11	2, 12, 14	2, 8, 10	1, 14, 15
7, 8, 15	3, 9, 10	3, 12, 15	4, 8, 12	1, 10, 11	4, 11, 15	4, 9, 13
5, 9, 12	6, 8, 14	5, 11, 14	3, 13, 14	5, 8, 13	1, 12, 13	3, 8, 11
6, 11, 13	7, 11, 12	7, 10, 13	5, 10, 15	6, 9, 15	7, 9, 14	6, 10, 12

Notice that the seven blocks in the first row make up a $(7, 3, 1)$-design. This is no coincidence. Since lines of a spread cannot intersect, and every pair of lines in a projective plane must intersect, it follows that the set of lines of a $PG(2, 2)$ inside our $PG(3, 2)$ must all lie in different spreads (that is, different columns of our table). The points across the top lie in the projective plane (isomorphic to $PG(2, 2)$) that is obtained by looking at all projective points of $PG(3, 2)$ whose first homogeneous coordinate is 0. You can verify that the set of such vectors forms a 3-dimensional vector space over $GF(2)$ and therefore serves as a model for the projective plane $PG(2, 2)$. As an exercise, consider the projective plane (isomorphic to $PG(2, 2)$) obtained from the points whose *last* homogeneous coordinate is 0. These points are represented by the even integers. Verify that each of the lines contained in this plane lies in a different column of our table. In other words, each column contains exactly one entry composed of all even integers.

Now, we have two ways to describe Kirkman's Fifteen Young Ladies: the spreads in $PG(3, 2)$ and the subfields of an algebraic number field. By a $KS(15)$, we mean a resolvable $(15, 3, 1)$ block design. As we have seen, the quadratic (varieties) and biquadratic (blocks) subfields of the degree-16 algebraic number field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$ form a $KS(15)$.

But wait—there's more. The points in $PG(3, 2)$ are 4-digit bit strings. There is a one-to-one correspondence (prove it!) between the points in $PG(3, 2)$ and the quadratic subfields of K, defined by mapping the nonzero bit string $b_1b_2b_3b_4$ to the quadratic subfield $\mathbb{Q}(\sqrt{2^{b_1}3^{b_2}5^{b_3}7^{b_4}})$. Let's see how this correspondence acts on a KS(15) design.

A set of three points in $PG(3, 2)$, such as $\{0110, 1101, 1011\}$, are collinear provided their vector sum over the 2-element field $GF(2)$ is the zero vector. This follows from the fact that projective lines are defined as 2-dimensional subspaces. Recall that a "line" or "block" in the extension-field version of the $KS(15)$ design is a set of three quadratic subfields $\{\mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{q}), \mathbb{Q}(\sqrt{r})\}$ that belong to the same biquadratic subfield of K. We would like to find conditions on p, q, and r that force this to occur. Necessarily, we would require $\sqrt{r} \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$, $\sqrt{p} \in \mathbb{Q}(\sqrt{q}, \sqrt{r})$, and $\sqrt{q} \in \mathbb{Q}(\sqrt{p}, \sqrt{r})$. In other words, the biquadratic subfields determined by any two of $\{p, q, r\}$ are all the same. This boils down to a fairly simple condition on the variables. The condition that the subfields $\{\mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{q}), \mathbb{Q}(\sqrt{r})\}$ lie in a common biquadratic subfield is that p, q, and r are nonsquare integers whose product

is a square. For instance, the three quadratic subfields $\{\mathbb{Q}(\sqrt{15}), \mathbb{Q}(\sqrt{42}), \mathbb{Q}(\sqrt{70})\}$ lie in a unique biquadratic subfield since $15 \cdot 42 \cdot 70 = 44100 = 210^2$ is a square. A little algebra shows that three 4-dimensional vectors $\{a, b, c\}$ representing points in $PG(3, 2)$ sum to zero mod 2 if and only if their corresponding quadratic subfields $\{\mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{q}), \mathbb{Q}(\sqrt{r})\}$ have the property that pqr is a square. To see this, note that a vector sum of zero for $a \oplus b \oplus c$ translates to an even number of 1s summed in each of the four coordinate positions. In the field model, this means that each exponent of $2^{b_1}3^{b_2}5^{b_3}7^{b_4}$ is even and so the entire product is a square. Thus, the correspondence preserves lines, and so is an isomorphism between the set of 35 lines of a $KS(15)$ in $PG(3, 2)$ and its corresponding $KS(15)$ in K.

At this point you probably will not be surprised that Kirkman's famous design arises in two more seemingly unrelated areas of mathematics, namely recreational mathematics and the very applied area of coding theory. So, let's talk about Kirkman's design and how it relates to a certain guessing game involving fifteen players wearing hats.

Fifteen schoolgirls, fifteen hats

Here is a famous problem in recreational mathematics that we'll call the Three Hats Game. Three players enter a room and a maroon or orange hat is placed on each person's head. The color of each hat is determined by a coin toss, with the outcome of one coin toss having no effect on the others. Each person can see the other players' hats but not his own.

No communication of any sort is allowed, except for an initial strategy session before the game begins. Once players have had a chance to look at the other hats, they must simultaneously guess the color of their own hats or pass. The group shares a hypothetical $3 million prize if at least one player guesses correctly and no players guess incorrectly. The problem is to find a strategy whereby the group's chance of winning exceeds 50%.

Mathematicians credit the Three Hats Game to Todd Ebert, a computer scientist, who introduced it in his Ph.D. thesis in 1998 [**9**]. The problem was then popularized by an April 2001 article in the *New York Times* [**18**].

The winning strategy is as follows. Each player looks at the other two hats. A player who sees two of the same color guesses the *missing* color. A player who sees two different colors passes. Now there are eight ways of distributing hats of two colors among three distinct players. In six of these ways, two players see hats of different colors and they pass; the third player sees two hats of the same color, guesses the missing color—and that turns out to be a win. In the other two cases, all hats are the same color; each player guesses the missing color, and all three are wrong. Hence, the strategy works in six of eight cases, and so the three players will win 3/4 of the time. This comes as a surprise to most readers.

We will see how this technique generalizes, with increasingly better odds, to any number of players of the form $2^n - 1$ for $n \geq 3$. In particular, it generalizes to a situation where there are $2^4 - 1 = 15$ players—maybe even fifteen schoolgirls—and the analysis involves a mathematical middle-man known as a Hamming Code. So, before we describe the general technique, let's talk about error-correcting codes.

Some coding theory 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. These researchers saw the need for something 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 code words form a subspace of $\mathbb{Z}_q^n$, the n-dimensional vector space over $\mathbb{Z}_q$, the integers mod q. A basis for such a linear code is called a *generating set* for the code. One way to describe such a set is with a *generator matrix*, which is a q-ary matrix of n columns whose rows generate the code.

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 $D(1101000, 0011010) = 4$. 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 "far apart" in the Hamming distance sense, they can detect errors. Even better, if we assume that only a few errors occur, 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 and will successfully correct a single error. 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*.

Hamming's first error correcting scheme was a perfect 1-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 1-error correcting codes of minimum distance 3 for all $n \geq 2$. These are now known as the Hamming codes, and they include both Hamming's original $(7, 4)$ code and the $(3, 1)$ triplication code.

Here is the connection between the Kirkman Schoolgirls Problem and Hamming codes. As we have seen, the 35 triples in TABLE 4 are the 35 blocks of a resolvable $(15, 3, 1)$-design, and the numbers $1, \ldots, 15$ are the varieties. The incidence matrix M for this design is a 35×15 matrix of zeros and ones. It is straightforward to show that the *row space* of M—that is, the vector space generated by the rows of M—is an 11-dimensional subspace of $\mathbb{Z}_2^{15}$, and that this subspace is a $(15, 11)$ Hamming code.

We now show how Hamming codes are the keys to understanding the winning strategy for the Three Hats Game, and how the Kirkman Schoolgirls problem is linked to the Fifteen Hats Game.

Fifteen schoolgirls, fifteen hats: A solution. Go back and look at the Three Hats Game again. Notice that the triplication code contains two codewords and six blocks with errors. The six erroneous blocks correspond to the six winning hat placements for the three players, and the two codewords correspond to the two losing hat placements. As we see in what follows, that is not an accident.

Here is how a solution to the Kirkman Schoolgirls problem leads to a solution to the Fifteen Hats Game in which the probability of winning is much greater than 50%: in fact, it is well over 90%.

First, we number the girls from 1 to 15 in the same way that they are labeled in TABLE 4. We think of these as 4-digit nonzero binary numbers.

Now, suppose that the girls enter the room, each obtaining a hat, and circle up in order 1 through 15. Each player now does the following. She looks at the numbers corresponding to each girl wearing a maroon hat, and she computes the corresponding vector sum. For example, if girls 1, 3, 5, 8, 10, 12, and 14 are wearing maroon hats, then girl 4 will compute $1 \oplus 3 \oplus 5 \oplus 8 \oplus 10 \oplus 12 \oplus 14$. As a mod-2 vector sum, this is

$$0001 \oplus 0011 \oplus 0101 \oplus 1000 \oplus 1010 \oplus 1100 \oplus 1110 = 0111, \text{ or } 7.$$

1. If that sum is equal to her number, she guesses that her color is orange.
2. If that sum is equal to zero, she guesses that her color is maroon.
3. If neither of these two situations occurs, she passes.

Let's analyze what happens. First suppose that the sequence of all maroon hats corresponds to a vector sum of 0. Then every schoolgirl falls into one of the first two cases. All of them will guess incorrectly, and the team loses. More precisely, if a particular girl has on a maroon hat, the corresponding sum that she computes will be equal to her number. So, she will fall into case 1 above and will therefore guess that her hat is orange. Wrong! A similar mistake occurs if the girl is wearing orange.

Next, suppose that the sequence of all maroon hats corresponds to a vector sum of $n \neq 0$. Girl k sees a vector sum of $n \oplus k$ or n, according as she is wearing maroon or orange, respectively. If $k \neq n$, then what Girl k sees is neither her own number nor zero, so she passes. Girl n, however, sees 0 if she is wearing maroon and sees n if she is wearing orange; in both of these cases, she guesses correctly and the team wins.

In the previous example, in which the sequence of all maroon hats corresponds to a vector sum of $7 \neq 0$, the only girl to see either 0 or her own number is Girl 7, who sees 7. That is her own number so she correctly guesses that her hat is orange, and the team wins.

As an exercise, suppose that girls 1, 4, 6, 8, 9, 10, and 12 are wearing maroon hats, and the others are wearing orange hats. Is this a winning configuration, and if so, which girl makes the correct guess? The solution is at the end of the next section.

Why does this work? This is where Hamming codes point the way. The reason is that the configurations of maroon hats with vector sums of 0 are in one-to-one correspondence with the binary vectors of length 15 in the row space of M, the incidence matrix of the Kirkman (15, 3, 1)-design, and as previously mentioned, this row space forms a (15, 11) Hamming code. Recall that the Hamming codes are perfect codes with minimum distance 3. This means that every vector in the entire vector space $\mathbb{Z}_2^{15}$ either (a) is a codeword, or (b) differs in one coordinate from a unique Hamming codeword. That is, changing just one special coordinate position of a vector that is *not* a codeword will leave us with a codeword. Thus, in an arrangement of hats not corresponding to a codeword, the only one who can detect this is the girl who occupies that

special coordinate position. She can tell what her hat color should be in order to make the entire configuration a codeword—and so she guesses the opposite color.

As for the probability of winning with this strategy, it is 15/16, and here is why: We have seen that the triples corresponding to the Kirkman Schoolgirls problem generate a vector space, the row space of the incidence matrix M, that corresponds to the (15, 11) Hamming code. The incorrect guesses will occur exactly when the arrangements of maroon hats correspond to a vector in the Hamming code. Hence, the probability that the players lose the game is given by the size of the Hamming code divided by the total number of $\mathbb{Z}_2$-vectors of length 15. This gives us $2^{11}/2^{15} = 1/16$. So the chances of winning are actually $1 - 1/16$, or 15/16. We hope you find this as surprising as we do. By increasing the number of players, you actually *increase* your chances of winning.

As for the Three Hats Game, the triplication code is a (3, 1) Hamming code. Its generator matrix is [1 1 1], the set of codewords is {000, 111} and there are 8 binary vectors of length 3. Hence, the probability of a win is $1 - 1/4$, or 3/4.

With that, we leave Thomas Kirkman and his fifteen schoolgirls, whose simple arrangement question has led us into many varied areas of mathematics. Hats off to all fifteen of you!

Questions

Where can I find out more about Kirkman designs and block designs in general? One of the best places to begin is Chapter 6 of Kenneth Bogart's beautifully written book [**3**], which will take you a fair way into the subject. Two others are Marshall Hall's classic [**12**] and the more technical book by Beth, Jungnickel, and Lenz [**1**], both of which are excellent and will take you as far as you want to go.

Is the Kirkman design found in $PG(3, 2)$ the only solution to Kirkman's Schoolgirls Problem? We say that two block designs are *isomorphic* if there is a 1-1 correspondence between the two sets of varieties that is also a 1-1 correspondence between the two sets of blocks. It was known for a long time that there are eighty nonisomorphic (15, 3, 1)-designs. In 1922, F. N. Cole [**7**] proved that only four of these eighty designs are resolvable. Cole also proved that three of these have two nonisomorphic resolutions, while the fourth has only one. (Exercise: Determine whether the (15, 3, 1)-design presented in this paper has a resolution not isomorphic to the one in TABLE 2.)

For which values of v do resolvable $(v, 3, 1)$-designs exist? This question dates back to Kirkman himself [**15, 16**] and was open for over a hundred years. Finally, in 1971 D. K. Ray-Choudhury and R. M. Wilson proved that resolvable $(v, 3, 1)$-designs exist if and only if $v \equiv 3 \bmod 6$ [**17**] .

Are there Kirkman designs in number fields other than the degree-16 field described above? Yes. Let $n > 3$ and let $p_1, p_2, \ldots, p_n$ be distinct primes. The field $L_n = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$ is an extension of degree 2^n over the rational numbers $\mathbb{Q}$. In such fields, the quadratic and the biquadratic subfields of L_n are the varieties and blocks, respectively, of a resolvable $(2^n - 1, 3, 1)$-design. As an exercise, show that such a design contains $b = (2^n - 1)(2^{n-1} - 1)/3$ blocks, and each variety appears in $r = 2^{n-1} - 1$ blocks. A more challenging exercise is to show that these designs are resolvable.

The set of 15 Schoolgirls contains 455 3-element subsets, or trios. Suppose the school term is 13 weeks long. What if the Schoolgirls wanted to arrange 13 weeks' worth of walks so that each trio of girls can walk together exactly once during the term? They can do it. Note that this amounts to partitioning the 455 trios into 13

distinct Kirkman (15, 3, 1)-designs. Evidently, in 1850 Cayley referred to Kirkman's original problem as well as to Sylvester's extension to 13 walks. In 1974, R. H. F. Denniston briefly discussed the problem's history, and then presented a solution [**8**]. As an exercise, find a partition of the 84 3-element subsets of $\{1, \ldots, 9\}$ into seven resolvable (9, 3, 1)-designs. Happy walking!

The Schoolgirl Problem connects block designs, finite projective geometries, algebraic number fields, error-correcting codes, and recreational mathematics. Are there any other connections? Yes, there is at least one more connection. The set $G_K = (\mathbb{Z}/2\mathbb{Z})^4 = \{(a, b, c, d) : a, b, c, d \in 0, 1\}$ is a group under the operation of coordinate-wise addition mod 2. This group, $(\mathbb{Z}/2\mathbb{Z})^4$, has 15 subgroups of order 2, 35 subgroups of order 4 and 15 subgroups of order 8; each order-2 subgroup is contained in three order-4 subgroups and seven order-8 subgroups. (Does this sound familiar?) In fact, G_K is what is known as the *Galois group* of the degree-16 field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$. It is the group of isomorphisms of K to itself that leaves $\mathbb{Q}$ fixed. There is a one-to-one, order-reversing correspondence between the subfields of K and the subgroups of G_K, and the details of this correspondence are laid out in the Fundamental Theorem of Galois Theory, one of the most beautiful theorems in mathematics.

What about the solution to that exercise? We know that girls 1, 4, 6, 8, 9, 10, and 12 are wearing maroon hats, and the others are wearing orange hats. The sequence of all maroon hats yields the vector sum $1 \oplus 4 \oplus 6 \oplus 8 \oplus 9 \oplus 10 \oplus 12$, that is,

$$0001 \oplus 0100 \oplus 0110 \oplus 1000 \oplus 1001 \oplus 1010 \oplus 1100 = 0100, \text{ or } 4.$$

Girl k sees $k \oplus 4$, and the only one with a winning view is Girl 4, who sees the all-zeros vector. Therefore, she guesses maroon, nobody else guesses, and the team wins.

REFERENCES

1. T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, 2nd ed., Cambridge University Press, 1999.
2. N. L. Biggs, T. P. Kirkman, mathematician, *Bull. London Math. Soc.* **13** (1981) 97–120.
3. K. P. Bogart, *Introductory Combinatorics*, 3rd ed., Harcourt Academic Press, 2000.
4. R. C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics* **9** (1939) 353–399.
5. E. Brown, The many names of (7, 3, 1), this MAGAZINE **75** (2002) 83–94.
6. A. Cayley, On the triadic arrangements of seven and fifteen things, *Philos. Mag.* **37**(3) (1850) 50–53.
7. F. N. Cole, Kirkman parades, *Bull. Amer. Math. Soc.* **28** (1922) 435–437.
8. R. H. F. Denniston, Sylvester's problem of the 15 schoolgirls, *Discrete Math.* **9** (1974) 229–233.
9. T. Ebert, Applications of recursive operators to randomness and complexity. Ph.D. Thesis, University of California at Santa Barbara, 1998.
10. R. A. Fisher, *The Design of Experiments*, Oliver and Boyd, Edinburgh, 1935.
11. R. A. Fisher, An examination of the different possible solutions of a problem in incomplete blocks, *Ann. Eugenics* **10** (1940), 52–57.
12. M. Hall, Jr., *Combinatorial Theory*, 9th ed., Blaisdell Publishing Company, 1967.
13. J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, 1998.
14. T. A. Kirkman, On a problem in combinations, *Camb. Dublin Math. J.* **2** (1847) 191–204.
15. ———, Query 6, *Lady's and Gentlemen's Diary* (1850) 48.
16. ———, Note on an unanswered prize question, *Camb. Dublin Math. J.* **5** (1850) 255–262.
17. D. K. Ray-Chaudhury and R. M. Wilson, Solution of Kirkman's schoolgirl problem, in *Combinatorics*, Proc. Sympos. Pure Math., vol. 19, AMS, 1971, pp. 187–203.
18. S. Robinson, Why mathematicians now care about their hat color, *The New York Times*, 10 April 2001.
19. J. J. Sylvester, Note on the historical origin of the unsymmetrical six-valued function of six letters, *Philos. Mag.* **21**(4) (1861) 369–377.
20. J. J. Sylvester, Note on a nine schoolgirls problem, *Messenger of Mathematics* **22** (1893) 159–160.
21. W. S. B. Woolhouse, Prize question 1733, *Lady's and Gentleman's Diary*, 1844.