involve

a journal of mathematics

New generalized secret-sharing schemes with points on a hyperplane using a Wronskian matrix

Weston Loucks and Bahattin Yildiz

msp

2020

vol. 13, no. 2

INVOLVE 13:2 (2020)
dx.doi.org/10.2140/involve.2020.13.257

New generalized secret-sharing schemes with points on a hyperplane using a Wronskian matrix

Weston Loucks and Bahattin Yildiz

(Communicated by Kenneth S. Berenhaut)

A new secret-sharing scheme is constructed using elementary tools from different fields of mathematics. A method is introduced which uses the assignment of points on a hyperplane, serving as terminal points of vectors which meet an outlined criterion for linear independence. Submatrices of a Wronskian matrix are used in the assignment of these points. This method is also generalized to include a weighted scheme and a multilevel hierarchical model.

1. Introduction

The first secret-sharing schemes were introduced by Shamir [1979] and Blakley [1979] independently. While Shamir used polynomial interpolation for the basis of his algorithm, Blakley used the intersection of hyperplanes to describe the secret-sharing scheme.

A secret-sharing scheme is a scheme where the key d (called the *secret*) is distributed by a *dealer* to a number of participants in such a way that allows only an authorized subset of participants (called an *access group*) to discover the secret. In a *fully democratic scheme*, n participants each receive a share of the secret and a threshold level of at least k of them must collaborate to recover it.

Since their inception, both Shamir's and Blakley's schemes have inspired other secret-sharing schemes which take different approaches to solving this problem or generalize it into more complex access structures. A *weighted scheme* allows certain individuals to have as much information as multiple participants. The number of shares a participant holds is referred to as their *weight*. A *multilevel hierarchy* requires a specific number of individuals to be present at various levels of a hierarchy, where participants at a higher level may replace those at a lower level but not vice versa. A *dictatorial scheme* is a special case of this model, where one or more participants must be required in all access groups. Different approaches have

MSC2010: primary 94A60; secondary 11T71, 34A30.
Keywords: secret-sharing schemes, hyperplane, Wronskian, hierarchical secret-sharing schemes, generalized cross product.

been employed to construct schemes that have these properties or other variants. For some of the work done in this context we refer the reader to [Benaloh and Leichter 1990; Beutelspacher and Vedder 1989; Brickell 1989; Charnes et al. 1997; Dawson and Donovan 1994; Ito et al. 1989; Lai and Ding 2004; Simmons 1990; 1992; Tassa 2007].

In this work, we describe a new approach to construct a secret-sharing scheme which uses points on a hyperplane as shares of information. Two main generalizations are explored with this scheme: the weighted scheme and the multilevel hierarchy. The fully democratic scheme is a special case of each of these models. Our proposed scheme uses elementary tools from an undergraduate curriculum and is accessible to readers with a limited technical background.

The rest of the work is organized as follows. In Section 2, we give the necessary preliminaries needed for our construction. In Section 3 we discuss how the dealer constructs a hyperplane equation to contain the secret. Section 4 describes how points may be found which allow for the hyperplane's equation to be reconstructed. Section 5 explains how participants would recover the equation of a hyperplane and discover the secret. Section 6 explains how a weighted scheme is implemented, and Section 8 explores the multilevel hierarchy. An example follows each generalization. Finally, Section 10 presents a proof for why a pair of assigned points will never be collinear with the secret when the threshold level of participants exceeds 2. We finish the paper with concluding remarks and directions for potential future research on the topic.

2. Preliminaries

As two distinct points define a unique line in $\mathbb{R}^2$, and three distinct points which are not collinear define a unique plane in $\mathbb{R}^3$, this method uses the principle that the terminal points of k distinct, linearly independent vectors define a unique hyperplane in $\mathbb{R}^k$. Consequently, taking one of these points as a *base point*, the vectors in the direction of the remaining $k-1$ points form $k-1$ linearly independent vectors which can be used to find a vector normal to the hyperplane.

A *k-dimensional hyperplane* is defined as the collection of points in $\mathbb{R}^k$ satisfying the equation

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = b, \tag{2-1}$$

where the constants $a_i \in \mathbb{R}$ are not all equal to zero and $b \in \mathbb{R}$. Each point $(x_1, x_2, \ldots, x_k)$ is in $\mathbb{R}^k$. A hyperplane, in general, is an *affine space* which has one fewer dimension than the ambient vector space in which it exists. An affine space, in this context, is a vector subspace which does not necessarily contain the origin point $\vec{O}$. For example, even though three points are required to define a plane in $\mathbb{R}^3$, only two linearly independent vectors are needed to define a 2-dimensional affine space of $\mathbb{R}^3$, which is a plane. If one has the knowledge of a point which lies on some plane, and two linearly independent vectors parallel to that plane, then one can define a plane in $\mathbb{R}^3$ and write its equation. The following vector will be normal to the hyperplane:

$$\vec{n} = [a_1 \ \ a_2 \ \ \cdots \ \ a_k]^\top. \tag{2-2}$$

For computational purposes in applications, a hyperplane will be constructed by the dealer such that $a_1, \ldots, a_k \in \mathbb{Z}_+$. Furthermore, the dealer will always set $a_k = 1$. In executing the scheme, participants will calculate a normal vector $\vec{N} = c\vec{n}$ for some $c \in \mathbb{R} \setminus \{0\}$. Since $a_k = 1$, they will divide $\vec{N}$ by its last component c to find $\vec{n}$.

If a point $P = (x_1, x_2, \ldots, x_k) \in \mathbb{R}^k$ satisfies (2-1), it *lies on the hyperplane*. The secret $d \in \mathbb{Z}$ will be associated with the x_1-intercept of the hyperplane. If $d = 0$ was never to be used as the secret, the dealer could simply set $b = a_1 d$, where d is the x_1-intercept directly. However, when $d = 0$, using this rule causes a problem when the hyperplane equation is being recovered by the participants. This problem is explained in Section 4. To allow 0 as a secret, the dealer can use a bijective mapping from $d \in \mathbb{Z}$ to $b \in \mathbb{Z} \setminus \{0\}$. The following mapping shall be used:

$$b = \begin{cases} a_1 d & \text{if } d > 0, \\ a_1(d-1) & \text{if } d \le 0. \end{cases} \tag{2-3}$$

Therefore, an x_1-intercept of -1 implies $d = 0$. In general, when the participants find an x_1-intercept with a negative value, they must add 1 to it to reveal the secret.

In a fully democratic scheme, each of the n participants holds the same level of information; any participant can be substituted in place of another. In this case, n distinct points that lie on the hyperplane will be assigned to n individuals, whereby any collection of k points defines the same hyperplane in $\mathbb{R}^k$, when expressed in the dealer's form ($a_k = 1$)

$$a_1 x_1 + a_2 x_2 + \cdots + a_{k-1} x_{k-1} + x_k = b. \tag{2-4}$$

3. Constructing a suitable hyperplane

A hyperplane can be generated with random parameters while retaining a fixed x_1-intercept at b/a_1. The dealer creates an equation of the form (2-4) with each integer coefficient a_i chosen randomly from the interval $(0, \max(|d|, n)]$ for $1 \le i < k$. This will generate an *askew hyperplane*, which has an intercept on each axis. A normal vector $\vec{n}$ created by the dealer has the form

$$\vec{n} = [a_1 \ \ a_2 \ \ \cdots \ \ a_{k-1} \ \ 1]^\top. \tag{3-1}$$

The vector $\vec{n}' \in \mathbb{R}^{k-1}$ is defined by the first $k-1$ components of (3-1). Let x_{j_i} denote the j-th coordinate of a point assigned to the i-th participant. By choosing 1 as the last component of $\vec{n}$, the dealer is then able to calculate x_{k_i} according to the formula

$$x_{k_i} = b - (a_1 x_{1_i} + a_2 x_{2_i} + \cdots + a_{k-1} x_{(k-1)_i}), \tag{3-2}$$

and x_{k_i} retains the randomness from (3-1). The coordinates $x_{1_i}, x_{2_i}, \ldots, x_{(k-1)_i}$ will be chosen from an *assignment matrix* presented in Section 4.

4. Assigning suitable points

If a system of random assignment were used for points on the hyperplane, it is possible that some collection of k points cannot be used to reconstruct the hyperplane's equation. For example, three points chosen randomly on a plane in $\mathbb{R}^3$ might be collinear. Therefore, a need arises for a systematic way to create a rectangular matrix of size $(k-1) \times n$, with $k \leq n$, whereby any collection of $k-1$ columns forms a basis for $\mathbb{R}^{k-1}$. This matrix shall be called the *assignment matrix A'*. In other words, A' should be constructed so that all submatrices of size $(k-1) \times (k-1)$ will be nonsingular. Applying (3-2) for each participant is comparable to appending an extra row to the bottom of the assignment matrix, creating a matrix of size $k \times n$; then, each column represents an assigned point on the hyperplane. This matrix shall be called the *augmented assignment matrix A*. All $k \times k$ submatrices of A must also be nonsingular.

Let A_{h*} represent the h-th row of A. Using elementary row operations

$$A_{k*} + a_1 A_{1*} + a_2 A_{2*} + a_3 A_{3*} + \cdots + a_{k-1} A_{(k-1)*} = [b \;\; b \;\; \cdots \;\; b]. \tag{4-1}$$

Due to (4-1), A' cannot have a row of 1s, or equivalently, a scalar multiple of such a row because all resulting A would be singular. Equation (4-1) also shows why $b = a_1 d$ cannot be used when $d = 0$.

One way to obtain matrices that satisfy the conditions that we want is by the use of *Wronskian matrices* arising from differential equations. In other words, A' can be taken as a submatrix of a certain Wronskian matrix W when $\det W \neq 0$ can be guaranteed under certain conditions. In general, when $\{y_1, y_2, \ldots, y_n\}$ form a fundamental set of solutions for an ordinary differential equation, the Wronskian matrix is defined as follows [Krusemeyer 1988]:

$$W(y_1, y_2, \ldots, y_n)(x) = \begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ \dfrac{d}{dx} y_1 & \dfrac{d}{dx} y_2 & \cdots & \dfrac{d}{dx} y_n \\ \dfrac{d^2}{dx^2} y_1 & \dfrac{d^2}{dx^2} y_2 & \cdots & \dfrac{d^2}{dx^2} y_n \\ \vdots & \vdots & \ddots & \vdots \\ \dfrac{d^{n-1}}{dx^{n-1}} y_1 & \dfrac{d^{n-1}}{dx^{n-1}} y_2 & \cdots & \dfrac{d^{n-1}}{dx^{n-1}} y_n \end{bmatrix}. \tag{4-2}$$

The first $k-1$ rows of such a matrix will be used for A'. The chosen input $x = x_0$ in (4-2) must guarantee a nonzero determinant for W and for all square submatrices coming from its first $k-1$ rows. Consequently, every subset of size $k-1$ from $\{y_1, y_2, \ldots, y_n\}$ must be a set of linearly independent solutions to some $(k-1)$-th order differential equation which can be evaluated at the same input x_0.

A special class of differential equations on real-valued functions yields a Wronskian matrix which has a nonzero determinant everywhere the functions are defined. Specifically, this is a property of the fundamental set of solutions to a linear, homogeneous differential equation with constant coefficients, or *LHCC* [Nijenhuis 1980].

An n-th order LHCC can be expressed in the form

$$c_n \frac{d^n y}{dx^n} + c_{n-1} \frac{d^{n-1} y}{dx^{n-1}} + \cdots + c_0 y = 0. \tag{4-3}$$

In differential operator notation, $D^n(y) = d^n y/dx^n$, with D being the differential operator on y with respect to x. The *characteristic polynomial form* is created by substituting a real-valued variable to the n-th power, r^n, in place of $D^n(y)$. Consequently, for each distinct real root r_i with $1 \le i \le n$, we know $y_i = e^{r_i x}$ is a fundamental solution for (4-3). Without constraint on the real-valued coefficients $c_1, c_2, \ldots, c_n$ it is possible to construct such a polynomial with exactly n real, distinct roots $r_1, r_2, \ldots, r_n$. Specifically, a differential equation can be written in operator notation as

$$[D - r_1][D - r_2][\cdots][D - r_n](y) = 0. \tag{4-4}$$

It is always possible for an n-th order LHCC to have n linearly independent solutions $y_1 = e^{r_1 x}$, $y_2 = e^{r_2 x}$, ..., $y_n = e^{r_n x}$ because it is always possible to construct (4-4) for any value of n. Note that the coefficients c_i would not be chosen by the dealer, but rather the roots r_i would be chosen. The coefficients in (4-3) may be calculated using *elementary symmetric polynomials*, but for the purposes of secret-sharing it is sufficient to note that (4-4) can be created for any collection of n real, distinct roots.

The Wronskian matrix from these functions at $x = 0$ results in the *Vandermonde matrix* [Pólya 1922]:

$$W(e^{r_1 x}, e^{r_2 x}, \ldots, e^{r_n x})(0) = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ r_1 & r_2 & \cdots & r_n \\ r_1^2 & r_2^2 & \cdots & r_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ r_1^{n-1} & r_2^{n-1} & \cdots & r_n^{n-1} \end{bmatrix}. \tag{4-5}$$

The determinant of this matrix is nonzero whenever $r_1, r_2, \ldots, r_n$ are distinct values [Rushanan 1989]. Evaluating W resulting from (4-4) at $x_0 \neq 0$ produces a matrix which will be equivalent to (4-5) after multiplying a scalar of $e^{-r_i x_0}$ to the i-th column, where $1 \leq i \leq n$ [Pólya 1922]. The Vandermonde matrix is an underlying feature of Shamir's scheme [1979], but appears as a result of polynomial interpolation rather than a Wronskian matrix [Lai and Ding 2004]. The connection between the Vandermonde matrix and the Wronskian matrix for LHCCs is noteworthy as a starting point for the results in this work. However, LHCCs on their own are not practicable for this scheme. Evaluation at $x_0 = 0$ results in a row of 1s, which is problematic when the augmented assignment matrix A is created; A will be singular. Evaluation at $x_0 \in \mathbb{Z} \setminus \{0\}$ yields entries which are not integers when $r_i \in \mathbb{Z}_+$. Integer entries are preferable for computing applications.

These issues can be resolved by using *Cauchy–Euler differential equations* instead of LHCCs. The form of these differential equations is related to that of LHCCs, using a change of variables $x = \ln(t)$ for $t > 0$ [Zill and Cullen 2006]:

$$c_n t^n \frac{d^n y}{dt^n} + c_{n-1} t^{n-1} \frac{d^{n-1} y}{dt^{n-1}} + \cdots + c_0 y = 0. \tag{4-6}$$

For each distinct real root r of a Cauchy–Euler differential equation, $y(t) = t^r$ is a solution. Each term of (4-6) can be computed for $0 < j \leq n$ [Zill and Cullen 2006]:

$$c_j t^j \frac{d^j y}{dt^j} = c_j r(r-1)(r-2)\cdots(r-j+1)t^r. \tag{4-7}$$

After applying (4-7) to each term in (4-6), t^r may be factored out. This leaves a polynomial in r, with each term having c_j as a leading coefficient. Since the dealer can calculate the values of each c_j from any chosen set of real, distinct roots r_i, some polynomial of degree n can always exist with n distinct roots. The dealer can construct a polynomial equation

$$(r - r_1)(r - r_2)\cdots(r - r_n) = 0.$$

Expanding this using elementary symmetric polynomials would reveal exactly what c_j values are necessary to achieve the desired roots. However, since such a polynomial can always exist in theory, the dealer would simply assume that a Cauchy–Euler differential equation exists with the desired roots, without explicitly calculating c_j values.

Let F be defined as the fundamental set of solutions to (4-6). Then, the following property holds regarding its Wronskian determinant [Zill and Cullen 2006]:

$$\det W(F)(t) \neq 0 \iff t \in (0, +\infty).$$

For this secret-sharing scheme, the dealer will use the Wronskian matrix W of F with distinct $r_i \in \mathbb{Z}_+$. Any resulting $(k-1) \times (k-1)$ submatrix taken from the first $k-1$ rows, evaluated at $t_0 \in (0, +\infty)$, will be nonsingular because the first row will constitute a fundamental set of solutions for some $(k-1)$-th order Cauchy–Euler differential equation. As a convention for standardizing point assignment, W will be evaluated at $t_0 = 2$, although any $t_0 \in \mathbb{Z}_+ \setminus \{1\}$ could be considered.

When each root r_i is distinct, the first $k-1$ rows of W lead to

$$A'(t) = \begin{bmatrix} t^{r_1} & t^{r_2} & \cdots & t^{r_n} \\ \frac{d}{dt}t^{r_1} & \frac{d}{dt}t^{r_2} & \cdots & \frac{d}{dt}t^{r_n} \\ \frac{d^2}{dt^2}t^{r_1} & \frac{d^2}{dt^2}t^{r_2} & \cdots & \frac{d^2}{dt^2}t^{r_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{d^{k-2}}{dt^{k-2}}t^{r_1} & \frac{d^{k-2}}{dt^{k-2}}t^{r_2} & \cdots & \frac{d^{k-2}}{dt^{k-2}}t^{r_n} \end{bmatrix}. \tag{4-8}$$

Since the dealer chooses each $r_i \in \mathbb{Z}_+$, the *permutation function* $P(n, j) = n!/(n-j)!$ may be utilized in the calculation of (4-8). For all t^r, with $r \in \mathbb{Z}_+$ such that $j \le r$,

$$\frac{d^j}{dt^j}t^r = P(n, j)t^{r-j}.$$

When $j > r$,

$$\frac{d^j}{dt^j}t^r = 0.$$

When each r_i is relatively small, many entries of (4-8) will be zero. However, determinants of $(k-1) \times (k-1)$ submatrices taken from the first $k-1$ rows will remain nonzero where $t_0 > 0$. In particular, a submatrix populated by a maximal amount of zero entries would present a worst-case scenario. It would result from the solution set $F_0 = \{1, t, t^2, \dots, t^{n-1}\}$. One might ask if $\det W(F_0)(t_0) \neq 0$.

From (4-2) the n-th row of W is populated by the $(n-1)$-th order derivatives. Specifically, this row would include

$$\frac{d^{n-1}}{dt^{n-1}}t^{n-1} = P(n-1, n-1) = (n-1)!\,.$$

$W(F_0)(t)$ is *upper-triangular*,

$$W(F_0)(t) = \begin{bmatrix} 1 & x & t^2 & \cdots & t^{n-1} \\ 0 & 1 & 2t & \cdots & P(n-1, 1)t^{n-2} \\ 0 & 0 & 2 & \cdots & P(n-1, 2)t^{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & P(n-1, n-1) \end{bmatrix}, \tag{4-9}$$

and

$$\det W(F_0)(t) = 0!\,1!\,2! \cdots (n-1)!\,. \tag{4-10}$$

In practice, the points generated by (4-9) would not be used in this secret-sharing scheme; it represents a theoretical scenario. Furthermore, if $1 \in F$ then $d = 1$ could never be used as it would give the secret directly to a participant. A systematic method of assigning each r_i using prime numbers, presented in Section 6, will be used instead. This method will be more advantageous for a weighted scheme and can be applied to the multilevel hierarchy as well.

4.1. ***Submatrices of A are nonsingular when constructed from Cauchy–Euler differential equations.*** Using the Wronskian matrix of Cauchy–Euler differential equations with distinct, real roots, all $(k-1) \times (k-1)$ submatrices of $A'(t)$ with $t \in \mathbb{Z}_+ \setminus \{1\}$ will be nonsingular. However, it is not immediately obvious that all $k \times k$ submatrices of A will be nonsingular after the extra row is appended using (3-2). Each entry in this row x_{k_i} will follow the formula

$$x_{k_i} = b - \left(a_1 t^{r_i} + a_2 \frac{d}{dt} t^{r_i} + \cdots + a_{k-1} \frac{d^{k-2}}{dt^{k-2}} t^{r_i} \right). \tag{4-11}$$

Therefore, $A(t)$ can be written as

$$A(t) = \begin{bmatrix} t^{r_1} & t^{r_2} & \cdots & t^{r_n} \\ \frac{d}{dt} t^{r_1} & \frac{d}{dt} t^{r_2} & \cdots & \frac{d}{dt} t^{r_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{d^{k-2}}{dt^{k-2}} t^{r_1} & \frac{d^{k-2}}{dt^{k-2}} t^{r_2} & \cdots & \frac{d^{k-2}}{dt^{k-2}} t^{r_n} \\ x_{k_1} & x_{k_2} & \cdots & x_{k_n} \end{bmatrix}. \tag{4-12}$$

We will show that any $k \times k$ submatrix of $A(t)$ is nonsingular when evaluated at $t_0 \in \mathbb{Z}_+ \setminus \{1\}$. Without loss of generality, define the submatrix A_k by the first k columns of (4-12). We will apply elementary row operations on A_k to arrive at a new matrix M. If we can prove that $\det M \neq 0$, then we can infer that A_k will be nonsingular. We will use the notation $A_k \sim B$ to indicate that the matrix B comes from using elementary row operations on A_k, and thus the matrices have equal rank.

Apply (4-1), and then multiply the k-th row by $1/b$ to get

$$A_k \sim \begin{bmatrix} t^{r_1} & t^{r_2} & \cdots & t^{r_k} \\ \frac{d}{dt} t^{r_1} & \frac{d}{dt} t^{r_2} & \cdots & \frac{d}{dt} t^{r_k} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{d^{k-2}}{dt^{k-2}} t^{r_1} & \frac{d^{k-2}}{dt^{k-2}} t^{r_2} & \cdots & \frac{d^{k-2}}{dt^{k-2}} t^{r_k} \\ 1 & 1 & \cdots & 1 \end{bmatrix}. \tag{4-13}$$

Swap rows until $[1\ \ 1\ \ \cdots\ \ 1]$ is the first row, and all following rows appear in their original order:

$$A_k \sim B = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ t^{r_1} & t^{r_2} & \cdots & t^{r_k} \\ \frac{d}{dt}t^{r_1} & \frac{d}{dt}t^{r_2} & \cdots & \frac{d}{dt}t^{r_k} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{d^{k-2}}{dt^{k-2}}t^{r_1} & \frac{d^{k-2}}{dt^{k-2}}t^{r_2} & \cdots & \frac{d^{k-2}}{dt^{k-2}}t^{r_k} \end{bmatrix}. \tag{4-14}$$

Perform the following row operations, where B_{hi} represents the entry of B on the h-th row, i-th column, and B_{h*} represents the h-th row of B:

$$\begin{gathered} B_{k*} - (B_{k1})B_{1*} \to B_{k*}, \\ B_{(k-1)*} - (B_{(k-1)1})B_{1*} \to B_{(k-1)*}, \\ \vdots \\ B_{2*} - (B_{21})B_{1*} \to B_{2*}. \end{gathered}$$

Then $A_k \sim B \sim M$, where

$$M = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & t^{r_2}-t^{r_1} & t^{r_3}-t^{r_1} & \cdots & t^{r_k}-t^{r_1} \\ 0 & \frac{d}{dt}t^{r_2}-\frac{d}{dt}t^{r_1} & \frac{d}{dt}t^{r_3}-\frac{d}{dt}t^{r_1} & \cdots & \frac{d}{dt}t^{r_k}-\frac{d}{dt}t^{r_1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \frac{d^{k-2}}{dt^{k-2}}t^{r_2}-\frac{d^{k-2}}{dt^{k-2}}t^{r_1} & \frac{d^{k-2}}{dt^{k-2}}t^{r_3}-\frac{d^{k-2}}{dt^{k-2}}t^{r_1} & \cdots & \frac{d^{k-2}}{dt^{k-2}}t^{r_k}-\frac{d^{k-2}}{dt^{k-2}}t^{r_1} \end{bmatrix}. \tag{4-15}$$

Observe that

$$\det M = \det \begin{bmatrix} t^{r_2}-t^{r_1} & t^{r_3}-t^{r_1} & \cdots & t^{r_k}-t^{r_1} \\ \frac{d}{dt}t^{r_2}-\frac{d}{dt}t^{r_1} & \frac{d}{dt}t^{r_3}-\frac{d}{dt}t^{r_1} & \cdots & \frac{d}{dt}t^{r_k}-\frac{d}{dt}t^{r_1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{d^{k-2}}{dt^{k-2}}t^{r_2}-\frac{d^{k-2}}{dt^{k-2}}t^{r_1} & \frac{d^{k-2}}{dt^{k-2}}t^{r_3}-\frac{d^{k-2}}{dt^{k-2}}t^{r_1} & \cdots & \frac{d^{k-2}}{dt^{k-2}}t^{r_k}-\frac{d^{k-2}}{dt^{k-2}}t^{r_1} \end{bmatrix}. \tag{4-16}$$

Let β_i for $i \in \{1, 2, \dots, k\}$ represent constant coefficients. Consider a Cauchy–Euler differential equation whose solution is

$$\begin{aligned} y(t) &= \beta_2(t^{r_2} - t^{r_1}) + \beta_3(t^{r_3} - t^{r_1}) + \cdots + \beta_k(t^{r_k} - t^{r_1}) \\ &= -(\beta_2 + \beta_3 + \cdots + \beta_k)t^{r_1} + \beta_2 t^{r_2} + \beta_3 t^{r_3} + \cdots + \beta_k t^{r_k}. \end{aligned}$$

This is a solution to a Cauchy–Euler differential equation where

$$c_1 = -(c_2 + c_3 + \cdots + c_k).$$

We may then consider (4-16) as a Wronskian determinant for a set of solutions $\{t^{r_2}-t^{r_1}, t^{r_3}-t^{r_1}, \dots, t^{r_k}-t^{r_1}\}$, which are linearly independent, since all the r_i are distinct. Therefore, $\det M \neq 0$ when $t_0 \in \mathbb{Z}_+ \setminus \{1\}$ and hence A_k is nonsingular.

5. Recovering the secret

When k points on a hyperplane are known, one point is chosen to be the base point, P_B. Then $k-1$ vectors $\vec{v}_1, \vec{v}_2, \dots, \vec{v}_{k-1}$ are calculated using P_B as the initial point and each of the remaining $k-1$ points as terminal points. Once $k-1$ vectors are known, the participants will find the *generalized cross product* $\bigwedge$ of these linearly independent vectors, resulting in a normal vector $\vec{N}$. Here, $\hat{e}_1 \in \mathbb{R}^k$ represents a unit basis vector with k components having 1 as the i-th component and 0 elsewhere:

$$\vec{N} = \bigwedge(\vec{v}_1, \dots, \vec{v}_{k-1}) = \det \begin{bmatrix} & \vec{v}_1 & \\ & \vec{v}_2 & \\ & \vdots & \\ & \vec{v}_{k-1} & \\ \hat{e}_1 & \hat{e}_2 \; \cdots & \hat{e}_k \end{bmatrix}. \tag{5-1}$$

$\vec{N}$ is parallel to $\vec{n}$, given in (3-1). To find $\vec{n}$, the participants divide $\vec{N}$ by its last component. Next, P_B is considered as a row vector $\vec{P_B}$. The equation of the hyperplane can be found:

$$[x_1 \;\; x_2 \;\; \cdots \;\; x_k]\,\vec{n} = \vec{P_B}\vec{n}. \tag{5-2}$$

Evaluating the products reveals (2-4). Finally, the participants set $x_2 = x_3 = \cdots = x_k = 0$ and solve the resulting equation for $x_1 = d$.

6. The weighted scheme

Instead of assigning each participant a single point, one could also assign a line, plane, or m-dimensional affine space that lies on the hyperplane in $\mathbb{R}^k$ with $m < k-1$. For example, someone who knows the equation of a line on the hyperplane has twice as much information as someone who only has a point. Generalizing this notion, the knowledge of an m-dimensional affine space is equivalent to knowing $m+1$ points that lie on the hyperplane. A point is regarded as a 0-dimensional affine space. These pieces of d, called *shadows*, [Ito et al. 1989] can be thought of in terms of geometric representations such as lines or affine spaces, but in practice will be assigned as a set S of points. The number of points in S is referred to as the weight of the shadow. Points that are already assigned cannot be reused.

In the weighted scheme, n does not represent the number of people involved, but rather the total weight of all assigned shadows, while k represents the threshold sum of weights needed to recover the secret. The case where every participant has only a weight-1 shadow is equivalent to the fully democratic scheme.

Without a defined system of organizing the points, issues may arise as new participants are added to the weighted scheme. For example, it would be difficult to know whether an arbitrary point P_i can be assigned to a new participant, or whether that point exists in S for an existing participant. Each person must have an infinite set of points on reserve, sharing a property unique to that person, so that those points will never be assigned to a different participant.

S_i will denote a shadow for the i-th participant. $P_{i,j}$ refers to the j-th point given to the i-th participant, $f_{i,j}$ refers to the solution of a Cauchy–Euler differential equation used to generate $P_{i,j}$, and p_i denotes the i-th prime number. A shadow of weight $m+1$ is defined as

$$\begin{aligned} S_i &= \{P_{i,1}, P_{i,2}, \dots, P_{i,m+1}\}, && 1 \le i \le n, m+1 < k, \\ f_{i,j} &= t^{p_i^j}, && 1 \le j \le m+1. \end{aligned} \tag{6-1}$$

This will allow each participant to have a reserve of points that can be used as shadows for that participant only.

7. Weighted scheme example

Suppose six people with a total shadow weight of $n = 10$ are given partial information, and a total shadow weight of $k = 5$, or greater, is needed to recover the secret $d = 9$.

The dealer chooses $k - 1 = 4$ random integers from (0, 10]: 6, 7, 7, 4. This is used to construct (3-1).

$$\vec{n} = [6 \;\; 7 \;\; 7 \;\; 4 \;\; 1]^\top.$$

The dealer calculates $a_1 d = 6 \cdot 9 = 54$. An equation of form (2-4) is created:

$$6x_1 + 7x_2 + 7x_3 + 4x_4 + x_5 = 54. \tag{7-1}$$

Next, the dealer must create $n = 10$ vectors in $\mathbb{R}^{k-1} = \mathbb{R}^4$ such that any set of four vectors is guaranteed to be linearly independent. For this task, a Wronskian matrix of a tenth order Cauchy–Euler differential equation is used.

Suppose there are six people entrusted to hold partial information about the secret: Alice, Bob, Carlos, David, Elif, and Fahad. Furthermore, suppose Alice has a shadow of weight 3 (a 2-dimensional affine space). Bob and Carlos both have shadows of weight 2 (a line), while David, Elif, and Fahad each have shadows of weight 1 (a point). To stay organized and identify which point belongs to whom, (6-1) is applied:

$$\begin{aligned} &f_{1,1} = t^2, && f_{1,2} = t^4, && f_{1,3} = t^8, && f_{2,1} = t^3, && f_{2,2} = t^9, \\ &f_{3,1} = t^5, && f_{3,2} = t^{25}, && f_{4,1} = t^7, && f_{5,1} = t^{11}, && f_{6,1} = t^{13}. \end{aligned} \tag{7-2}$$

The dealer considers the fundamental set of solutions F listed in (7-2). The Wronskian matrix is given by

$$W(F)(t)=\begin{bmatrix} t^2 & t^4 & t^8 & t^3 & t^9 & t^5 & t^{25} & \cdots & t^{13} \\ 2t & 4t^3 & 8t^7 & 3t^2 & 9t^8 & 5t^4 & 25t^{24} & \cdots & 13t^{12} \\ 2 & 12t^2 & 56t^6 & 6t & 72t^7 & 20t^3 & 600t^{23} & \cdots & 156t^{11} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 9! & 0 & P(25,9)t^{16} & \cdots & P(13,9)t^4 \end{bmatrix}. \qquad (7\text{-}3)$$

The first four rows of (7-3) are evaluated at $t=2$ to get the 4×10 submatrix

$$A'=\begin{bmatrix} 4 & 16 & 256 & 8 & 512 & 32 & 2^{25} & 128 & 2048 & 8192 \\ 4 & 32 & 1024 & 12 & 2304 & 80 & 25\cdot 2^{24} & 448 & 11\cdot 2^{10} & 13\cdot 2^{12} \\ 2 & 48 & 3584 & 12 & 9216 & 160 & 600\cdot 2^{23} & 1344 & 110\cdot 2^{9} & 156\cdot 2^{11} \\ 0 & 48 & 336\cdot 2^5 & 6 & 504\cdot 2^6 & 240 & P(25,3)2^{22} & 3360 & 990\cdot 2^8 & P(13,3)2^{10} \end{bmatrix}. \qquad (7\text{-}4)$$

Next, the dealer determines the x_5-value that will be associated with each column of (7-4) using (3-2). The points are then assigned as follows.

Alice:

$$P_{1,1}=(4,4,2,0,54-(4\cdot 6-4\cdot 7-2\cdot 7-0\cdot 4))=(4,4,2,0,-12),$$
$$P_{1,2}=(16,32,48,48,54-(16\cdot 6-32\cdot 7-48\cdot 7-48\cdot 4))=(16,32,48,48,-794),$$
$$P_{1,3}=(256,1024,3584,336\cdot 2^5,-76746).$$

Bob:

$$P_{2,1}=(8,\,12,\,12,\,6,\,54-(8\cdot 6-12\cdot 7-12\cdot 7-6\cdot 4))=(8,\,12,\,12,\,6,\,-186),$$
$$P_{2,2}=(512,\,2304,\,9216,\,504\cdot 2^6,\,-212682).$$

Carlos:

$$P_{3,1}=(32,\,80,\,160,\,240,\,-2778),$$
$$P_{3,2}=(2^{25},\,25\cdot 2^{24},\,600\cdot 2^{23},\,P(25,3)2^{22},\,-269895073738).$$

David:

$$P_{4,1}=(128,\,448,\,1344,\,990\cdot 2^8,\,-1027018).$$

Elif:

$$P_{5,1}=(2048,\,11\cdot 2^{10},\,110\cdot 2^9,\,990\cdot 2^8,\,-1499082).$$

Fahad:

$$P_{6,1}=(8192,\,13\cdot 2^{12},\,156\cdot 2^{11},\,P(13,3)2^{10},\,-9686986).$$

Suppose that Alice, David, and Elif must collaborate to recover the secret. Their total shadow weight $3+1+1=k$ is large enough to do so. The participants choose a base point, such as Alice's point $P_{1,1}$. Vectors are expressed starting from this point:

$$\begin{aligned}
\overrightarrow{P_{1,1}P_{1,2}} &= P_{1,2} - P_{1,1} = \langle 12, 28, 46, 48, -782\rangle,\\
\overrightarrow{P_{1,1}P_{1,3}} &= P_{1,3} - P_{1,1} = \langle 252, 1020, 3582, 10752, -76734\rangle,\\
\overrightarrow{P_{1,1}P_{4,1}} &= P_{4,1} - P_{1,1} = \langle 124, 444, 1342, 253440, -1027006\rangle,\\
\overrightarrow{P_{1,1}P_{5,1}} &= P_{5,1} - P_{1,1} = \langle 2044, 11260, 56318, 253440, -1499070\rangle.
\end{aligned}$$

The participants then use (5-1):

$$\vec{N} = \det \begin{bmatrix} 12 & 28 & 46 & 48 & -782 \\ 52 & 1020 & 3582 & 10752 & -76734 \\ 124 & 444 & 1342 & 253440 & -1027006 \\ 2044 & 11260 & 56318 & 253440 & -1499070 \\ \hat{e}_1 & \hat{e}_2 & \hat{e}_3 & \hat{e}_4 & \hat{e}_5 \end{bmatrix}. \tag{7-5}$$

Thus,

$$\vec{N} = \begin{bmatrix} -71428262068224 \\ -83332972412928 \\ -83332972412928 \\ -47618841378816 \\ -11904710344704 \end{bmatrix} = -11904710344704 \begin{bmatrix} 6 \\ 7 \\ 7 \\ 4 \\ 1 \end{bmatrix}. \tag{7-6}$$

After dividing by -11904710344704, the participants recover $\vec{n}$. $\vec{P_B}$ represents the row vector with the components of the base point $P_{1,1}$. Then, the participants apply (5-2) to find (7-1). They find the x_1-intercept by letting $x_2 = x_3 = x_4 = x_5 = 0$, which implies $6x_1 = 54$. Finally, they discover the secret $x_1 = 9$.

8. The multilevel hierarchy

Some organizations may wish to use a hierarchy of participants that require a specified number individuals from various levels of the hierarchy to be present. For example, consider a military organization which is structured so that *private officers* have the lowest level of security clearance, *corporals* are one level above private officers, *sergeants* are one level above corporals, and so on to the top security level. Suppose further that there is a military secret which can be recovered by k participants, from which at least α_1 must be corporals, α_2 must be sergeants, and in general at least α_j participants must be j levels above private officers. Additionally, someone at a higher level may substitute for someone lower on the hierarchy. For instance, a corporal may take the place of a private officer if needed and a sergeant may take the place of a corporal or a private officer. This model is equivalent to the fully democratic scheme if there is only one security level, treated as the top security level, requiring k participants to be present. This secret-sharing scheme may accommodate the multilevel hierarchy by making several modifications.

Firstly, instead of assigning a point to each individual on the lowest level of the hierarchy, each of these participants will instead receive a distinct vector parallel to the hyperplane. Then, each participant above the lowest level will be assigned a point on the lowest level's hyperplane, as well as a distinct vector parallel to it. In this way, higher level participants must be present to recover (2-4); without them, a group of private officers at best can find $\vec{n}$ but not $a_1 d$. As far as that group knows the hyperplane could pass through the origin; based on this information alone, d is as likely to be 0 as it is any other value.

Secondly, it requires secrets to be *nested*; for any participant who is assigned a point on a hyperplane, its *last coordinate* is kept secret (with the exception of the top security level). An unknown last coordinate becomes the secret x_1-intercept of a *different* hyperplane associated with the next higher security level. Each hyperplane will exist in a different vector space associated with each level of the hierarchy. Since each hyperplane can have only *one* x_1-intercept, a point with an unknown coordinate must be *shared*; it must be the *same* point for each participant who receives it. Any participant below the top security level is assigned a distinct vector parallel to the hyperplane associated with their level, instead of a point on it. Participants above the lowest level are assigned a point accompanied by a vector on all the hyperplanes associated with security levels below them. Finally, each participant at the top security level would know all coordinates of a *distinct* point that lies on their hyperplane; assignment of shares on the top level works as it does for the fully democratic scheme with respect to participants at the top level.

Recovering the secret begins on the top level. Once a hyperplane equation in each level is solved for its x_1-intercept, it reveals the unknown coordinate of a point one level below to be solved, until eventually the hyperplane equation on the lowest level can be recovered. Finding the x_1-intercept of that hyperplane reveals d.

As a consequence of the shared point, hyperplanes created by the dealer (with the exception of that at the top level) must have *one more dimension* than the number of participants in that access group. For example, consider the case where *three* participants are required, one of which must be a corporal. Then, two private officers hold distinct vectors parallel to their hyperplane, along with one corporal who holds a point on this hyperplane and his own distinct vector parallel to it. This describes a hyperplane defined by three vectors along with one point. However, in $\mathbb{R}^3$ only two vectors along with one point are needed to recover the hyperplane. Therefore, the dealer should instead create a hyperplane in $\mathbb{R}^4$ at the lowest level to accommodate the three participants. To generalize this, suppose k participants are required and the highest level in the hierarchy is T levels above the lowest. Let H_j

denote the hyperplane j security levels above the lowest level, with H_0 denoting the hyperplane at the lowest level:

$$H_0 \in \mathbb{R}^{k+1}, \quad H_1 \in \mathbb{R}^{\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_T+1}, \quad \cdots, \quad H_{T-1} \in \mathbb{R}^{\alpha_{T-1}+\alpha_T+1}, \quad H_T \in \mathbb{R}^{\alpha_T}.$$

A shared point will lie on $H_0, H_1, \ldots, H_{T-1}$ respectively. Since a point P_i generated by t^{p_i} is associated with the i-th participant, the shared points should be of a different form. It is sufficient to use the solution $f(t) = t$ to generate each shared point.

By d_{H_j} we denote the secret x_1-intercept on hyperplane H_j (the overall secret is $d = d_{H_0}$). The dealer can convert any point P_i to a vector $\vec{v}_i$ parallel to a hyperplane by using the point $(0, 0, \ldots, a_1 d_{H_j})$ as the initial point for $\vec{v}_i$:

$$\vec{v}_i = P_i - (0, 0, \ldots, a_1 d_{H_j}). \tag{8-1}$$

Let the i-th column of A' be denoted by A'_{*i}. Subtracting $a_1 d_{H_j}$ from (3-2) we get

$$x_{k_i} - a_1 d_{H_j} = (a_1 d_{H_j} - (A'_{*i})^T \vec{n}') - a_1 d_{H_j} = -(A'_{*i})^T \vec{n}'.$$

Therefore,

$$\vec{v}_i = \left[t^{p_i} \;\; \frac{d}{dt} t^{p_i} \;\; \frac{d}{dt^2} t^{p_i} \;\; \cdots \;\; \frac{d}{dt^{k-1}} t^{p_i} \;\; -(A'_{*i})^T \vec{n}' \right]^\top. \tag{8-2}$$

9. Multilevel hierarchy example

A secret $d = 331$ is shared with $n = 8$ people, such that $k = 6$ participants must collaborate to recover the secret. Furthermore, among these six participants there must be at least $\alpha_1 = 3$ corporals and $\alpha_2 = 2$ sergeants at the top security level. The remaining participant may be a private officer at the lowest security level. Suppose the eight people are ranked as follows, with their respective Cauchy–Euler solutions in parentheses: *Private* Alice (t^2), *Private* Bob (t^3), *Corporal* Carlos (t^5), *Corporal* David (t^7), *Corporal* Elif (t^{11}), *Sergeant* Fahad (t^{13}), *Sergeant* Garret (t^{17}), *Sergeant* Hanna (t^{19}).

The dealer considers three vector spaces, one for each security level, which will each contain a single hyperplane H_0, H_1, H_2 respectively:

$$H_0 \in \mathbb{R}^{k+1} = \mathbb{R}^7, \quad H_1 \in \mathbb{R}^{\alpha_1+\alpha_2+1} = \mathbb{R}^6, \quad H_2 \in \mathbb{R}^{\alpha_2} = \mathbb{R}^2.$$

In constructing $H_0 \in \mathbb{R}^7$, the dealer randomly chooses $7 - 1 = 6$ integers from (0,331]: 256, 154, 306, 207, 111, 151. By $\vec{n}_{H_0}$ we denote the normal vector for H_0. Then

$$\vec{n}'_{H_0} = [256 \;\; 154 \;\; 306 \;\; 207 \;\; 111 \;\; 151]^\top,$$
$$\vec{n}_{H_0} = [256 \;\; 154 \;\; 306 \;\; 207 \;\; 111 \;\; 151 \;\; 1]^\top.$$

After calculating $a_1 d = 256 \cdot 331 = 84736$, the dealer writes the equation for H_0:

$$256x_1 + 154x_2 + 306x_3 + 207x_4 + 111x_5 + 151x_6 + x_7 = 84736. \tag{9-1}$$

There are eight to receive information, along with an additional shared point generated by $f(t) = t$, so the dealer uses a Wronskian matrix of size 9×9. However, only the first $7 - 1 = 6$ rows will be used for H_0, the first $6 - 1 = 5$ rows for H_1, and the first $2 - 1 = 1$ row for H_2. The last column will be used for a shared point by the higher-level participants on H_0 and H_1. Each of the other columns corresponds with a distinct participant, generated by their Cauchy–Euler solution and its derivatives:

$$W(F)(t) = \begin{bmatrix} t^2 & t^3 & t^5 & t^7 & \cdots & t^{19} & t \\ 2t & 3t^2 & 5t^4 & 7t^6 & \cdots & 19t^{18} & 1 \\ 2 & 6t & 20t^3 & 42t^5 & \cdots & 342t^{17} & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & 0 & \cdots & P(19,8)t^{12} & 0 \end{bmatrix}. \tag{9-2}$$

$W(F)(2)$ is evaluated, and the first $\mathbf{7} - 1 = 6$ rows define the assignment matrix A':

$$A' = \begin{bmatrix} 4 & 8 & 32 & 128 & \cdots & 2^{19} & 2 \\ 4 & 12 & 80 & 448 & \cdots & 19 \cdot 2^{18} & 1 \\ 2 & 12 & 160 & 1344 & \cdots & 342 \cdot 2^{17} & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 5! & 10080 & \cdots & P(19,5) \cdot 2^{14} & 0 \end{bmatrix}. \tag{9-3}$$

Using the last column of A', each of the corporals and sergeants knows a point lies on H_0 of the form (2,1,0,0,0,0,d_{H_1}). The private officers have no knowledge about H_1. Applying (8-2), the dealer determines a vector $\vec{v}_{i,H_0}$ parallel to H_0, which is assigned to the i-th participant:

$$\begin{aligned} \vec{v}_{1,H_0} &= \langle 4, 4, 2, 0, 0, 0, -A'^{T}_{*1}\vec{n}'_{H_0} \rangle \\ &= \langle 4, 4, 2, \dots, -(4{\cdot}256{+}4{\cdot}154{+}2{\cdot}306{+}0{\cdot}207{+}0{\cdot}111{+}0{\cdot}151) \rangle \\ &= \langle 4, 4, 2, 0, 0, 0, -2252 \rangle, \end{aligned}$$

$$\vec{v}_{2,H_0} = \langle 8, 12, 12, 6, 0, 0, -A'^{T}_{*2}\vec{n}'_{H_0} \rangle = \langle 8, 12, 12, 6, 0, 0, -8810 \rangle,$$

$$\begin{aligned} \vec{v}_{3,H_0} &= \langle 32, 80, 160, 240, 240, 120, -A'^{T}_{*3}\vec{n}'_{H_0} \rangle \\ &= \langle 32, 80, 160, 240, 240, 120, -163912 \rangle, \end{aligned}$$

$$\vec{v}_{4,H_0} = \langle 128, 448, 1344, 3360, 6720, 10080, -3476544 \rangle,$$

$$\vec{v}_{5,H_0} = \langle 2^{11}, 11{\cdot}2^{10}, 110{\cdot}2^{9}, 990{\cdot}2^{8}, 7920{\cdot}2^{7}, 55440{\cdot}2^{6}, -720254464 \rangle,$$

$$\vec{v}_{6,H_0} = \langle 2^{13}, P(13,1)2^{12}, P(13,2)2^{11}, P(13,3)2^{10}, P(13,4)2^{9}, P(13,5)2^{8}, -7417067520\rangle,$$

$$\vec{v}_{7,H_0} = \langle 2^{17}, P(17,1)2^{16}, P(17,2)2^{15}, P(17,3)2^{14}, P(17,4)2^{13}, P(17,5)2^{12}, -527980036096\rangle,$$

$$\vec{v}_{8,H_0} = \langle 2^{19}, P(19,1)2^{18}, P(19,2)2^{17}, P(19,3)2^{16}, P(19,4)2^{15}, P(19,5)2^{14}, -3883940315136\rangle.$$

The dealer creates an equation for $H_1 \in \mathbb{R}^6$ and calculates vectors parallel to this hyperplane in a similar manner. Each corporal and sergeant will be assigned a vector parallel to H_1. This hyperplane will have d_{H_1} as its x_1-intercept.

The point (2, 1, 0, 0, 0, 0, d_{H_1}) lies on H_0. The dealer uses this fact to calculate its value:

$$d_{H_1} = 84736 - (256\cdot 2 + 154\cdot 1 + 306\cdot 0 + 207\cdot 0 + 111\cdot 0 + 151\cdot 0) = 84070.$$

By $\vec{n}_{H_1}$ we denote the normal vector for H_1. The dealer chooses $6-1=5$ random integers from (0,331] for its first five components, using 1 as its last component:

$$\vec{n}'_{H_1} = [86\ \ 237\ \ 156\ \ 158\ \ 72]^{\top},$$
$$\vec{n}_{H_1} = [86\ \ 237\ \ 156\ \ 158\ \ 72\ \ 1]^{\top}.$$

After calculating $a_1 d_{H_1} = 86\cdot 84070 = 7230020$, the equation for H_1 can be written as

$$86x_1 + 237x_2 + 156x_3 + 158x_4 + 72x_5 + x_6 = 7230020. \tag{9-4}$$

Let A'' be defined by the first five rows of A', given in (9-3). The dealer uses $\vec{n}'_{H_1}$ and A'' to determine vectors parallel to H_1 by applying (8-2). From the last column of A'', each sergeant knows a point lies on H_1 of the form (2, 1, 0, 0, 0, d_{H_2}). The corporals have no knowledge about H_2. Vectors v_{i,H_1} parallel to H_1 are assigned to each corporal and sergeant:

$$\begin{aligned}\vec{v}_{3,H_1} &= \langle 32, 80, 160, 240, 240, -A''^{T}_{*3}\vec{n}'_{H_1}\rangle\\ &= \langle 32, 80, \dots, -(32\cdot 86+80\cdot 237+160\cdot 156+240\cdot 158+240\cdot 72)\rangle,\\ &= \langle 32, 80, 160, 240, 240, -101872\rangle,\end{aligned}$$

$$\begin{aligned}\vec{v}_{4,H_1} &= \langle 128, 448, 1344, 3360, 6720, -A''^{T}_{*4}\vec{n}'_{H_1}\rangle\\ &= \langle 128, 448, 1344, 3360, 6720, -1341568\rangle,\end{aligned}$$

$$\vec{v}_{5,H_1} = \langle 2^{11}, 11\cdot 2^{10}, 110\cdot 2^{9}, 990\cdot 2^{8}, 7920\cdot 2^{7}, -124665856\rangle,$$

$$\vec{v}_{6,H_1} = \langle 2^{13}, P(13,1)2^{12}, P(13,2)2^{11}, P(13,3)2^{10}, P(13,4)2^{9}, -973385728\rangle,$$

$$\vec{v}_{7,H_1} = \langle 2^{17}, P(17,1)2^{16}, P(17,2)2^{15}, P(17,3)2^{14}, P(17,4)2^{13}, -45918257152\rangle,$$

$$\vec{v}_{8,H_1} = \langle 2^{19}, P(19,1)2^{18}, P(19,2)2^{17}, P(19,3)2^{16}, P(19,4)2^{15}, -287891783680\rangle.$$

The dealer creates an equation for $H_2 \in \mathbb{R}^2$ and calculates *points* on this top-security-level hyperplane. Each sergeant will be assigned a point on H_2.

The point $(2, 1, 0, 0, 0, d_{H_2})$ lies on H_1. The dealer uses this fact to calculate its value:

$$d_{H_2} = 7230020 - (86 \cdot 2 + 237 \cdot 1 + 156 \cdot 0 + 158 \cdot 0 + 72 \cdot 0) = 7229611.$$

The dealer chooses $2 - 1 = 1$ random integers from (0,331]:

$$\vec{n}'_{H_2} = [33], \quad \vec{n}_{H_2} = \begin{bmatrix} 33 \\ 1 \end{bmatrix}.$$

After calculating $a_1 d_{H_2} = 33 \cdot 7229611 = 238577163$, the equation for H_2 can be written as

$$33x_1 + x_2 = 238577163. \tag{9-5}$$

The x_1-value for each sergeant comes from each of their respective entries on the first row of A'. These values, along with (9-5), are used to determine their respective x_2-values. Points P_{i,H_2} are assigned to each sergeant:

$$\begin{aligned}
P_{6,H_2} &= (2^{13}, 238577163 - 33 \cdot 2^{13}) = (2^{13}, 238306827),\\
P_{7,H_2} &= (2^{17}, 238577163 - 33 \cdot 2^{17}) = (2^{17}, 234251787),\\
P_{8,H_2} &= (2^{19}, 238577163 - 33 \cdot 2^{19}) = (2^{19}, 221275659).
\end{aligned}$$

Suppose *Private* Bob, *Corporal* Carlos, *Corporal* David, *Corporal* Elif, *Sergeant* Fahad, and *Sergeant* Garret must recover the secret $d = 331$. These participants meet the necessary conditions, in number and security level, to recover it.

First the two sergeants collaborate to find d_{H_2}. They start by finding a vector:

$$\overrightarrow{P_{6,H_2} P_{7,H_2}} = P_{7,H_2} - P_{6,H_2} = \langle 122880, -4055040\rangle.$$

They calculate a normal vector $\vec{N}_{H_2}$ for H_2:

$$\vec{N}_{H_2} = \det \begin{bmatrix} 122880 & -4055040 \\ \hat{e}_1 & \hat{e}_2 \end{bmatrix} = 4055040\hat{e}_1 + 122880\hat{e}_2 = 122880 \begin{bmatrix} 33 \\ 1 \end{bmatrix}. \tag{9-6}$$

Dividing by 122880 reveals $\vec{n}_{H_2}$. The sergeants define $\vec{P}_B$ as a row vector whose components are those of P_{6,H_2}, the base point of $\overrightarrow{P_{6,H_2} P_{7,H_2}}$. Then, using (5-2) they find the equation of H_2 (9-5). They find the x_1-intercept of H_2, which reveals $d_{H_2} = 7229611$. Now they know $P_{H_1} = (2, 1, 0, 0, 0, 7229611)$ lies on H_1.

Using their two vectors on H_1, they collaborate with the three corporals to consider five vectors parallel to H_1: $\vec{v}_{3,H_1}, \vec{v}_{4,H_1}, \vec{v}_{5,H_1}, \vec{v}_{6,H_1}, \vec{v}_{7,H_1}$. They apply (5-1) to calculate $\vec{N}_{H_1}$:

$$\vec{N}_{H_1} = \det \begin{bmatrix} & & \vec{v}_{3,H_1} & & & \\ & & \vec{v}_{4,H_1} & & & \\ & & \vec{v}_{5,H_1} & & & \\ & & \vec{v}_{6,H_1} & & & \\ & & \vec{v}_{7,H_1} & & & \\ \hat{e}_1 & \hat{e}_2 & \hat{e}_3 & \hat{e}_4 & \hat{e}_5 & \hat{e}_6 \end{bmatrix}$$

$$= \begin{bmatrix} 1003906400136412004352 0 \\ 27665792654922051747840 \\ 18210395165265147985920 \\ 18443861769948034498560 \\ 8404797768583914455040 \\ 1167333023414432563 20 \end{bmatrix} = 1167333023414432563 20 \begin{bmatrix} 86 \\ 237 \\ 156 \\ 158 \\ 72 \\ 1 \end{bmatrix}.$$

Dividing by 116733302341443256320 reveals $\vec{n}_{H_1}$. Then, the sergeants and corporals collectively define $\vec{P}_B$ as a row vector with the components of P_{H_1} and apply (5-2) to discover the equation for H_1 (9-4). Solving for its x_1-intercept reveals $d_{H_1} = 84070$. They now know that $P_{H_0} = (2, 1, 0, 0, 0, 0, 84070)$ lies on H_0.

They collaborate with *Private* Bob to consider six vectors parallel to H_0:

$$\vec{v}_{2,H_0}, \quad \vec{v}_{3,H_0}, \quad \vec{v}_{4,H_0}, \quad \vec{v}_{5,H_0}, \quad \vec{v}_{6,H_0}, \quad \vec{v}_{7,H_0}.$$

They apply (5-1) to find $\vec{N}_{H_0}$, a normal vector for H_0. They divide this vector by its last component to find $\vec{n}_{H_0}$. The participants define $\vec{P}_B$ as a row vector with the components of P_{H_0} and apply (5-2) to find the equation for H_0 (9-1). Finally, they solve this for its x_1-intercept, revealing the secret $d = 331$.

10. Eliminating a potential problem

If two points were assigned on a hyperplane such that they are collinear with the x_1-intercept when $k > 2$, it would be possible for the security of the scheme to be compromised. A line through these points, intersecting the x_1-intercept, would reveal the secret preemptively. However, it can be proven algebraically that this is impossible using the method presented (4-8) for point assignment when $k > 3$. For the case $k = 3$, the dealer can make sure that this does not happen by a careful assignment of shares.

Case 1: Assume that $k = 3$. Note that for $p_i \in \mathbb{Z}_+$ we have $(d/dt)t^{p_i} = p_i t^{p_i - 1}$. Without loss of generality we assume $p_2 > p_1$ and that the dealer chooses these values so that $p_1(b/a_1)$ is not divisible by t. Define three points as follows:

$$\begin{aligned} A &= (t^{p_1},\, p_1 t^{p_1-1},\, b - a_1 t^{p_1} - a_2 p_1 t^{p_1-1}),\\ B &= (t^{p_2},\, p_2 t^{p_2-1},\, b - a_1 t^{p_2} - a_2 p_2 t^{p_2-1}),\\ C &= (b/a_1, 0, 0). \end{aligned}$$

Assume A, B, C are distinct, collinear points. Then $\overrightarrow{CA} = u\overrightarrow{CB}$ for some $u \in \mathbb{R}\backslash\{0\}$. Let:

(I) $t^{p_1} - b/a_1 = u(t^{p_2} - b/a_1)$.

(II) $p_1 t^{p_1-1} = u p_2 t^{p_2-1}$.

(III) $b - a_1 t^{p_1} - a_2 p_1 t^{p_1-1} = u(b - a_1 t^{p_2} - a_2 p_2 t^{p_2-1})$.

From (I) and (II) and assuming $t \neq 0$,

$$u(t^{p_2} - b/a_1)(p_2 t^{p_2-1})t = (t^{p_1} - b/a_1)(p_2 t^{p_2-1})t = (t^{p_2} - b/a_1)(p_1 t^{p_1-1})t,$$

which gives

$$(t^{p_1} - b/a_1)(p_2 t^{p_2}) = (t^{p_2} - b/a_1)(p_1 t^{p_1}),$$

implying

$$p_2 t^{p_1+p_2} - (b/a_1) p_2 t^{p_2} = p_1 t^{p_1+p_2} - (b/a_1) p_1 t^{p_1}.$$

Add $(b/a_1) p_2 t^{p_2} - p_1 t^{p_1+p_2}$ to both sides and factor out the common factors:

$$t^{p_1+p_2}(p_2 - p_1) = (b/a_1)(p_2 t^{p_2} - p_1 t^{p_1}).$$

Canceling out t^{p_1} from both sides we get

$$t^{p_2}(p_2 - p_1) - (b/a_1) p_2 t^{p_2-p_1} = -(b/a_1) p_1.$$

This is a contradiction because the left-hand side is divisible by t, whereas the right-hand side is not.

Case 2: Assume that $k > 3$. Then $p_i \geq 2$ implies

$$\frac{d}{dt} t^{p_i} = p_i t^{p_i-1}, \quad \frac{d^2}{dt^2} t^{p_i} = p_i(p_i - 1) t^{p_i-2}.$$

Define three points as follows such that $p_1 \neq p_2$ and each $x_i \in \mathbb{R}$:

$$\begin{aligned} A &= \left(t^{p_1},\, p_1 t^{p_1-1},\, p_1(p_1-1)t^{p_1-2}, \dots, b - \left(a_1 t^{p_1} + \cdots + a_{k-1} \frac{d}{dt^{k-2}} t^{p_1}\right)\right),\\ B &= \left(t^{p_2},\, p_1 t^{p_2-1},\, p_2(p_2-1)t^{p_2-2}, \dots, b - \left(a_1 t^{p_2} + \cdots + a_{k-1} \frac{d}{dt^{k-2}} t^{p_2}\right)\right),\\ C &= (x_1, 0, 0, x_4, \dots, x_k). \end{aligned}$$

Assume A, B, C are distinct, collinear points. Note that the x_1-intercept is a point of the form C. Consider points on the line through A and B. For some $u_0 \in \mathbb{R}$, since its second and third components are zero, point C implies

$$\begin{aligned} p_1 t^{p_1-1} + (p_2 t^{p_2-1} - p_1 t^{p_1-1})u_0 &= 0, \\ p_1(p_1-1)t^{p_1-2} + (p_2(p_2-1)t^{p_2-2} - p_1(p_1-1)t^{p_1-2})u_0 &= 0, \end{aligned}$$

from which we get

$$\begin{aligned} &u_0(p_2 t^{p_2-1} - p_1 t^{p_1-1})(p_2(p_2-1)t^{p_2-2} - p_1(p_1-1)t^{p_1-2}) \\ &\qquad = -p_1 t^{p_1-1}(p_2(p_2-1)t^{p_2-2} - p_1(p_1-1)t^{p_1-2}) \\ &\qquad = -p_1(p_1-1)t^{p_1-2}(p_2 t^{p_2-1} - p_1 t^{p_1-1}). \end{aligned}$$

Thus,

$$\begin{aligned} & t^{p_1-1}(p_2(p_2-1)t^{p_2-2} - p_1(p_1-1)t^{p_1-2}) = (p_1-1)t^{p_1-2}(p_2 t^{p_2-1} - p_1 t^{p_1-1}) \\ \Longrightarrow\ & p_2(p_2-1)t^{p_1+p_2-3} - p_1(p_1-1)t^{2p_1-3} = (p_1-1)(p_2 t^{p_1+p_2-3} - p_1 t^{2p_1-3}) \\ \Longrightarrow\ & p_2(p_2-1)t^{p_1+p_2-3} - p_1(p_1-1)t^{2p_1-3} = p_2(p_1-1)t^{p_1+p_2-3} - p_1(p_1-1)t^{2p_1-3} \\ \Longrightarrow\ & p_2(p_2-1) = p_2(p_1-1) \\ \Longrightarrow\ & p_1 = p_2. \end{aligned}$$

This is a contradiction, since $p_1 \neq p_2$.

11. Conclusion

Secret-sharing schemes are great examples of how elementary mathematical ideas can be used to construct systems that can have profound application areas. Since their first appearance, they have been studied extensively from many directions, with the two main goals being constructing new schemes and finding application areas for the existing ones. In this paper we were able to use elementary mathematical ideas from an undergraduate curriculum to construct generalized secret-sharing schemes including the multilevel hierarchical ones. Our approach and the tools we have used are accessible to students and readers with limited technical background and they differ from the more complex approaches that have been used in the literature.

A detailed security cryptanalysis of the scheme can be done as part of a future research project. Due to the similarity of the tools used, we expect the security of the scheme to be similar to Shamir's scheme. Several attacks are possible, especially when the secret is chosen to be a small number. We propose a few countermeasures to the attacks. The first one is an obvious one, that is, choosing a large number and making the scheme more complex (with a complex hierarchy and distribution of shares if possible). Our second approach is inspired by code-based schemes. Instead of letting the secret be a single number, we could let $S = (S_1, S_2, \ldots, S_n)$

be the secret; i.e., the secret is an ordered n-tuple of *subsecrets*, where for each subsecret we apply the scheme to define shares. While this would increase the computational complexity of the scheme, it will be much more secure because to find the secret, every coordinate has to be found correctly. The probability of a successful attack will approach zero by increasing n. A possible direction for future research is to find practical areas in cryptography and information security in which our schemes can be implemented together with a detailed security and computational analysis.

Acknowledgement

The authors would like to thank the anonymous referees for their valuable comments and suggestions that helped improve the paper profoundly.

References

[Benaloh and Leichter 1990] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions", pp. 27–35 in *Advances in cryptology—CRYPTO '88* (Santa Barbara, CA, 1988), edited by S. Goldwasser, Lecture Notes in Comput. Sci. **403**, Springer, 1990. MR Zbl

[Beutelspacher and Vedder 1989] A. Beutelspacher and K. Vedder, "Geometric structures as threshold schemes", pp. 255–268 in *Cryptography and coding* (Cirencester, 1986), edited by H. J. Beker and F. C. Piper, Inst. Math. Appl. Conf. Ser. New Ser. **20**, Oxford Univ. Press, 1989. MR

[Blakley 1979] G. Blakley, "Safeguarding cryptographic keys", pp. 313–318 in *International workshop on managing requirements knowledge* (New York, 1979), AFIPS Conference Proceedings **48**, AFIPS, Montvale, NJ, 1979.

[Brickell 1989] E. F. Brickell, "Some ideal secret sharing schemes", *J. Combin. Math. Combin. Comput.* **6** (1989), 105–113. MR Zbl

[Charnes et al. 1997] C. Charnes, K. Martin, J. Pieprzyk, and R. Safavi-Naini, "Secret sharing in hierarchical groups", pp. 81–86 in *ICICS 1997: information and communications security*, Lecture Notes in Computer Science **1334**, Springer, 1997. Zbl

[Dawson and Donovan 1994] E. Dawson and D. Donovan, "The breadth of Shamir's secret-sharing scheme", *Comput. and Secur.* **13**:1 (1994), 69–78.

[Ito et al. 1989] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure", *Electron. Comm. Japan Part III Fund. Electron. Sci.* **72**:9 (1989), 56–63. MR

[Krusemeyer 1988] M. Krusemeyer, "The teaching of mathematics: why does the Wronskian work?", *Amer. Math. Monthly* **95**:1 (1988), 46–49. MR Zbl

[Lai and Ding 2004] C.-P. Lai and C. Ding, "Several generalizations of Shamir's secret sharing scheme", *Internat. J. Found. Comput. Sci.* **15**:2 (2004), 445–458. MR Zbl

[Nijenhuis 1980] A. Nijenhuis, "Complete solutions of linear difference equations", *Amer. Math. Monthly* **87**:8 (1980), 658–660. MR Zbl

[Pólya 1922] G. Pólya, "On the mean-value theorem corresponding to a given linear homogeneous differential equation", *Trans. Amer. Math. Soc.* **24**:4 (1922), 312–324. MR

[Rushanan 1989] J. J. Rushanan, "On the Vandermonde matrix", *Amer. Math. Monthly* **96**:10 (1989), 921–924. MR Zbl

[Shamir 1979] A. Shamir, "How to share a secret", *Comm. ACM* **22**:11 (1979), 612–613. MR Zbl

[Simmons 1990] G. J. Simmons, "How to (really) share a secret", pp. 390–448 in *Advances in cryptology—CRYPTO '88* (Santa Barbara, CA, 1988), edited by S. Goldwasser, Lecture Notes in Comput. Sci. **403**, Springer, 1990. MR

[Simmons 1992] G. J. Simmons, "An introduction to shared secret and/or shared control schemes and their application", pp. 441–497 in *Contemporary cryptology*, edited by G. J. Simmons, IEEE, New York, 1992. MR

[Tassa 2007] T. Tassa, "Hierarchical threshold secret sharing", *J. Cryptology* **20**:2 (2007), 237–264. MR Zbl

[Zill and Cullen 2006] D. G. Zill and M. R. Cullen, *Advanced engineering mathematics*, 3rd ed., Jones & Bartlett, Sudbury, MA, 2006.

Received: 2019-04-19 Revised: 2019-12-16 Accepted: 2020-02-24

wloucks@gmail.com
Department of Mathematics and Statistics,
Northern Arizona University, Flagstaff, AZ, United States

bahattin.yildiz@nau.edu
Department of Mathematics and Statistics,
Northern Arizona University, Flagstaff, AZ, United States

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

PRODUCTION

Silvio Levy, Scientific Editor

Cover: Alex Scorpan

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2020 is US $205/year for the electronic version, and $275/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2020 vol. 13 no. 2

Arithmetic functions of higher-order primes 181
KYLE CZARNECKI AND ANDREW GIDDINGS

Spherical half-designs of high order 193
DANIEL HUGHES AND SHAYNE WALDRON

A series of series topologies on $\mathbb{N}$ 205
JASON DEVITO AND ZACHARY PARKER

Discrete Morse functions, vector fields, and homological sequences on trees 219
IAN RAND AND NICHOLAS A. SCOVILLE

An explicit third-order one-step method for autonomous scalar initial value problems of first order based on quadratic Taylor approximation 231
THOMAS KRAINER AND CHENZHANG ZHOU

New generalized secret-sharing schemes with points on a hyperplane using a Wronskian matrix 257
WESTON LOUCKS AND BAHATTIN YILDIZ

Generalized Cantor functions: random function iteration 281
JORDAN ARMSTRONG AND LISBETH SCHAUBROECK

Numerical semigroup tree of multiplicities 4 and 5 301
ABBY GRECO, JESSE LANSFORD AND MICHAEL STEWARD

Enumerating diagonalizable matrices over $\mathbb{Z}_{p^k}$ 323
CATHERINE FALVEY, HEEWON HAH, WILLIAM SHEPPARD, BRIAN SITTINGER AND RICO VICENTE

On arithmetical structures on complete graphs 345
ZACHARY HARRIS AND JOEL LOUWSMA

Connectedness of digraphs from quadratic polynomials 357
SIJI CHEN AND SHENG CHEN