1-1-1996

Combinatorics and Campus Security

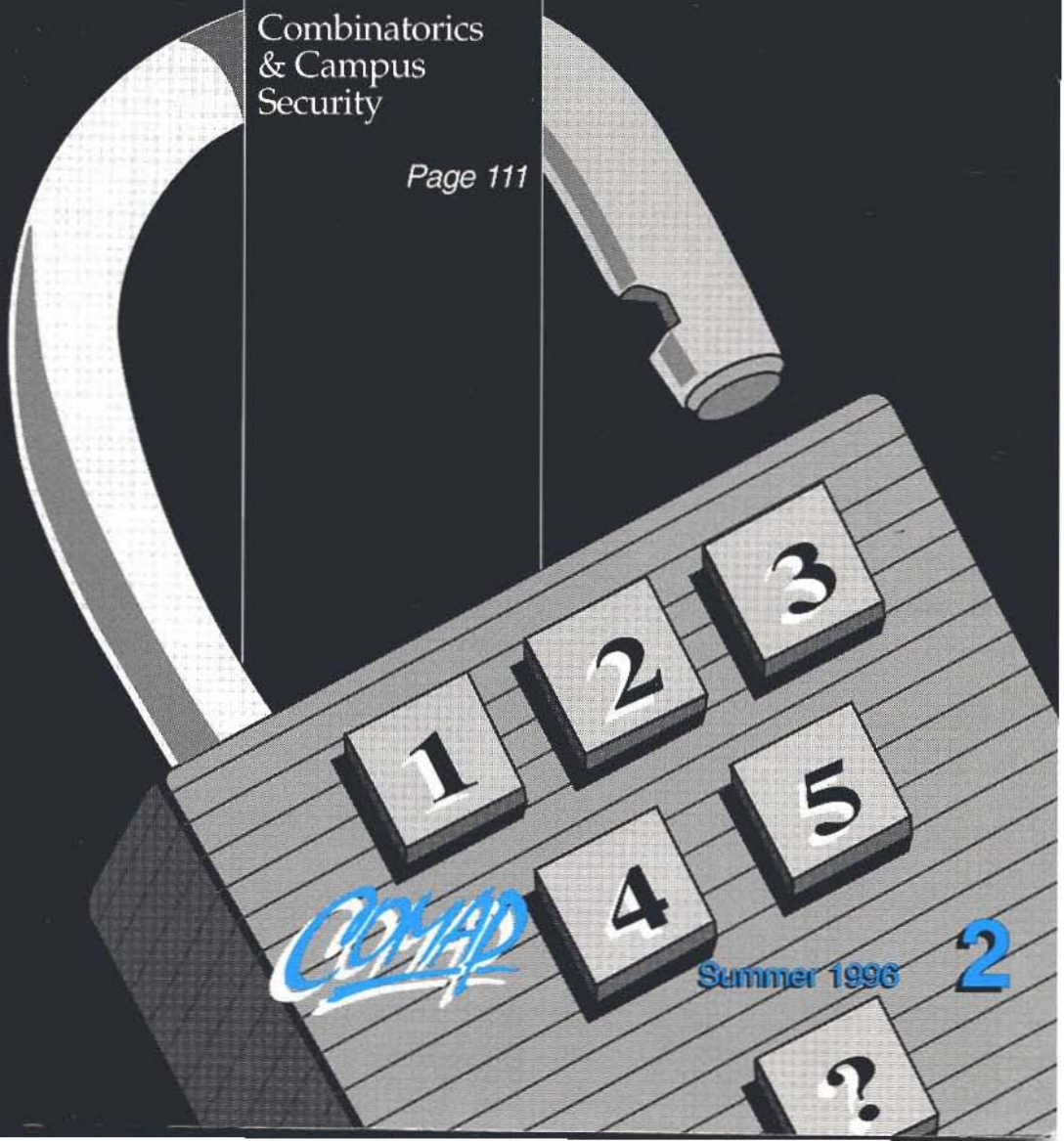
Arthur T. Benjamin
Harvey Mudd College

The UMAP Journal

The Journal of Undergraduate Mathematics and Its Applications

Combinatorics & Campus Security

Page 111



COMAP

Summer 1996 2

Combinatorics and Campus Security

Arthur T. Benjamin
Mathematics Dept.
Harvey Mudd College
Claremont, CA 91711
benjamin@hmc.edu

Introduction

One day I received electronic mail from our director of campus security [Gilbraith 1993]:

> I have a puzzle for you that has practical applications for me. I need to know how many different combinations there are for our combination locks. A lock has 5 buttons. In setting the combination you can use only 1 button or as many as 5. Buttons may be pressed simultaneously and/or successively, but the same button cannot be used more than once in the same combination.
>
> I had a student (obviously not a math major) email me that there are only 120 possibilities, but even I know this is only if you press all five buttons one at a time. It doesn't take into account 1–23–4–5, for instance. My question to you is how many combinations exist, and is it enough to keep our buildings adequately protected?

To clarify, combinations like 1–25–4 (which is the same as 1–52–4 but different from 4–25–1) and 1–2–5–43 are legal, whereas 13–35 is illegal because the number 3 is used twice. I gave this problem to the students in my discrete mathematics class as a bonus exercise. Most arrived at the (correct) answer of 1081 or 1082 by breaking the problem into oodles of cases, but this would not have been a convenient method if the locks contained 10 buttons instead of 5. I use this problem as an excuse to demonstrate the power of generating functions by solving the n-button problem. Most students are amazed that the problem is essentially *solved* by the function $e^x/(2-e^x)$, which leads to a surprisingly accurate approximation of $n!/(\ln 2)^{n+1}$.

For $n \geq 0$, we define A_n to be the number of solutions to the n-button problem. We define $A_0 = 1$ (interpreted as a busted lock—just open the door!) and therefore $A_1 = 2$ (either the lock is busted or press 1 to enter). Likewise, we can verify by brute force that $A_2 = 6$ and $A_3 = 26$. In general (for $n \geq 1$), we can determine A_n by a simple recursion. How many legal combinations begin by pressing k different buttons simultaneously? Once we choose which k buttons to push initially, there are A_{n-k} legal combinations that use the remaining $n-k$ buttons—hence there are $\binom{n}{k}A_{n-k}$ such combinations. This argument only works when $k \geq 1$, since if $k = 0$, then there is only one possibility—the

busted lock. It follows that $A_n = 1 + \sum_{k=1}^{n} \binom{n}{k} A_{n-k}$. Since $\binom{n}{k} = \binom{n}{n-k}$, we can rewrite the recurrence more conveniently. For $n \geq 0$,

$$A_n = 1 + \sum_{k=0}^{n-1} \binom{n}{k} A_k. \tag{1}$$

Note that when $n = 0$, the summation is empty and therefore equal to zero. Using **(1)**, we compute $A_4 = 150$, $A_5 = 1082$, $A_6 = 9366$, $A_7 = 94,586$, $A_8 = 1,091,670$, $A_9 = 14,174,522$, $A_{10} = 204,495,126$. With only 1082 combinations in the 5-button problem, a patient thief could easily enter one of the locked doors in under 2 hours (and less than an hour on average), so we recommend investing in a security system with at least 7 buttons. Ten buttons would offer more possibilities but would probably result in more people writing down the combination than committing it to memory! The 5-button lock compares most unfavorably with standard 40-number combination locks (which ought to be called *permutation* locks!) with $(40)^3 = 64,000$ possibilities.

Can we find a simple formula for A_n? Yes and no.

Generating Functions

For any sequence of numbers $a_0, a_1, a_2, \ldots$, we define the *ordinary generating function* to be the function

$$a(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots.$$

Amazingly, these series often simplify for certain (real or complex) values of x.

Example. The constant sequence $1, 1, 1, 1, \ldots$ has

$$a(x) = 1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x}$$

for $|x| < 1$.

Example. The *geometric* sequence $1, 3, 9, 27, \ldots$ has

$$a(x) = 1 + 3x + 9x^2 + 27x^3 + \cdots = \frac{1}{1-3x}$$

for $|x| < \frac{1}{3}$.

Example. The *binomial* sequence $1, 4, 6, 4, 1, 0, 0, \ldots$ has

$$a(x) = 1 + 4x + 6x^2 + 4x^3 + x^4 = (1+x)^4$$

for all x.

Example. The *Fibonacci* sequence $0, 1, 1, 2, 3, 5, 8, \ldots$ has

$$F(x) = 0 + x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + \cdots = \frac{x}{1 - x - x^2}$$

for $|x| < \frac{1}{\phi} \approx .618\ldots$, where $\phi = \frac{1+\sqrt{5}}{2} \approx 1.618\ldots$.

The simplification of the last example is left as an exercise (*after* reading this article) and can be found in most combinatorics textbooks (e.g., Tucker [1984]). In each series, the radius of convergence is determined by finding the absolute value of the smallest *singularity* of the simplified function. In the examples above, the first two functions have singularities at $x = 1$ and $x = \frac{1}{3}$, respectively. The third function has no singularities, and the last function has singularities at $x = \frac{1}{\phi}$ and $x = -\phi$. The radius of convergence will ultimately tell us the asymptotic growth rate of the coefficients of our sequence.

Next we define the *exponential generating function* of a sequence $a_0, a_1, a_2, \ldots$ to be the function

$$\hat{a}(x) = a_0 + a_1 x + a_2 \frac{x^2}{2!} + a_3 \frac{x^3}{3!} + \cdots,$$

which frequently simplifies for many combinatorial sequences. The following examples will be of interest to us:

Example. The sequence $1, 1, 1, 1, \ldots$ has

$$\hat{a}(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = e^x$$

for all x.

Example. The sequence $0, 1, 1, 1, \ldots$ has

$$\hat{a}(x) = x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = e^x - 1$$

for all x.

Example. The *lock sequence* $1, 2, 6, 26, \ldots$ has

$$\hat{A}(x) = 1 + 2x + 6\frac{x^2}{2!} + 26\frac{x^3}{3!} + \cdots,$$

which we endeavor to simplify.

Multiplying ordinary generating functions is just like polynomial multiplication, namely,

$$a(x)b(x) = c(x) = \sum_{n \geq 0} c_n x^n,$$

where

$$c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

It follows (and should be done as an exercise) that when multiplying exponential generating functions, we have

$$\hat{a}(x)\hat{b}(x) = \hat{c}(x) = \sum_{n\geq 0} c_n \frac{x^n}{n!},$$

where

$$c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}.$$

Since our recurrence **(1)** contains this form (with $b_0 = 0$, and $b_i = 1$ for all $i \geq 1$), we may find a closed form for its exponential generating function.

Proposition. *For the lock sequence,* $\hat{A}(x) = \frac{e^x}{2-e^x}$.

Proof: By **(1)**, we have

$$\begin{aligned}
\hat{A}(x) &= \sum_{n\geq 0} A_n \frac{x^n}{n!} \\
&= \sum_{n\geq 0} \left[1 + \sum_{k=0}^{n-1} \binom{n}{k} A_k \right] \frac{x^n}{n!} \\
&= e^x + \sum_{n\geq 0} \sum_{k=0}^{n-1} \left[\binom{n}{k} A_k \cdot 1 \right] \frac{x^n}{n!} \\
&= e^x + \hat{A}(x)(e^x - 1).
\end{aligned}$$

The last equality is easier to see by going back from the expression in the last line to that in the preceding line. Consequently, $\hat{A}(x)(1 - (e^x - 1)) = e^x$, and the proposition follows. □

Asymptotics

How does this help us find A_n? It can be shown (see Wilf [1994]) that for most ordinary generating functions $a(x)$ with radius of convergence $0 < R < \infty$, a_n is approximately a constant times

$$\left(\frac{1}{R}\right)^n,$$

when n is large. For instance, our earlier ordinary generating function examples with radii of convergence 1, $\frac{1}{3}$, ∞, and $\frac{1}{\phi}$ have a_n equal to 1, 3^n, (and for large n) 0, and $\phi^n/\sqrt{5}$, respectively. For an *exponential* generating function with radius of convergence R, it follows that a_n is approximately a constant times

$$n!\left(\frac{1}{R}\right)^n.$$

For our generating function $\hat{A}(x)$, we have $R = \ln 2$, since $x = \ln 2$ is the singularity of smallest magnitude. (Since we are on the complex plane, other singularities exist at points of the form $x = \ln 2 + (2\pi i)k$ for integer k.) Thus,

$$A_n \approx cn!\left(\frac{1}{\ln 2}\right)^n.$$

To determine the constant c, we first find a constant d that makes our function

$$\frac{e^x}{2-e^x} \approx \frac{d}{x-\ln 2}$$

(in the neighborhood of $x = \ln 2$), a simple function whose only singularity occurs at $x = \ln 2$. By applying L'Hôpital's rule to the function

$$\frac{e^x(x-\ln 2)}{2-e^x},$$

we obtain $d = -1$. Therefore,

$$\frac{e^x}{2-e^x} \approx \frac{-1}{x-\ln 2} = \frac{\frac{1}{\ln 2}}{1-\frac{x}{\ln 2}},$$

which has x^n coefficient

$$\left(\frac{1}{\ln 2}\right)^{n+1}.$$

Thus,

$$A_n \approx \frac{n!}{(\ln 2)^{n+1}}.$$

Our approximation gives the exact answer (when rounded to the nearest integer) for all $n \leq 15$. Although this approximation can be improved further by a Laurent series (see Wilf [1994]), the error of our approximation is proportional to

$$n!\left(\frac{1}{R'}\right)^n,$$

where

$$R' = \sqrt{(\ln 2)^2 + (2\pi)^2} \approx 6.32$$

is the magnitude of the next smallest singularity. Hence, the relative error of approximation is proportional to

$$\left(\frac{R}{R'}\right)^n \approx (.11)^n,$$

which is relatively insignificant. What *is* significant, however (from the vantage point of my discrete mathematics students) is the role that analysis plays in solving a simply stated combinatorial problem.

Shortly after this article was submitted for publication, Velleman and Call [1995] obtained similar results using different methods. In their paper, they define a_n to be the number of solutions to the n-button problem that use all n buttons. For $n > 0$, a_n is exactly half of A_n, since we can find a one-to-one correspondence between solutions that don't use all their buttons with those that do. For any solution that presses k sets of buttons but doesn't use all of them, we associate the solution that presses $k+1$ sets of buttons, where the first k sets are the same and the $(k+1)$st set consists of all the unused buttons. For instance, in the 9-button problem, 3–14–59 would be associated with 3–14–59–2678. In practice, if the lock combination is not changed periodically, it is an easy matter to see which numbers are used in the solution, by examining the paint surrounding the base of the buttons!

Acknowledgment

I am especially grateful to Robert Gilbraith for suggesting this problem.

References

Gilbraith, Robert. 1993. Personal communication. December, 1993.

Tucker, Alan. 1984. *Applied Combinatorics*. New York: Wiley.

Velleman, Dan, and Greg Call. 1995. Permutation and combination locks. *Mathematics Magazine* 68: 243–253.

Wilf, Herbert S. 1994. *Generatingfunctionology*. San Diego, CA: Academic Press.

About the Author

Arthur Benjamin received a B.S. from Carnegie-Mellon University in applied mathematics and the M.S.E. and Ph.D. degrees in mathematical sciences from Johns Hopkins University. In 1988, he received the Nicholson Prize of the Operations Research Society of America for his paper "Graphs, maneuvers, and turnpikes" (*Operations Research* 18 (1990): 202–216). In addition to teaching mathematics at Harvey Mudd, he enjoys playing tournament backgammon, racing against calculators, and performing magic.