Elem. Math. 71 (2016) 69 – 83
0013-6018/16/020069-15
DOI 10.4171/EM/301

Elemente der Mathematik

Finding vector-space bases at random

Osvaldo Marrero

Osvaldo Marrero earned degrees from the University of Miami and from Yale University, where he was also a postdoctoral research fellow. Subsequently, he completed courses at the University of Minnesota and at the Université de Montréal. After holding various positions in academia and in industry, he is currently a professor at Villanova University. His publications include papers in epidemiology, mathematics, medicine, and statistics.

1 Introduction

Over the finite field $\mathbb{F}_q$ of q elements, we consider the vector space V of finite dimension n. Of course, for V we always have the standard basis

$$(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, \ldots, 0, 1),$$

so finding a basis is never a problem. Instead, we were curious about what happens when we search for a basis for V at random. While investigating this question, we used some unexpected and very interesting mathematics.

All finite fields having the same cardinality are isomorphic. The finite field $\mathbb{F}_q$ exists if and only if q is a prime power. The symbol q will only be used to denote the cardinality of the field $\mathbb{F}_q$; thus, q will always be a prime power. Also, we use the notation $\mathcal{Q} := (2, 3, 2^2, 5, 7, 2^3, 3^2, \ldots)$, the sequence of prime powers.

Eine Basis in einem gegebenen Vektorraum zu finden ist nicht immer einfach. Im Allgemeinen benötigt man für ein solches Unterfangen das Auswahlaxiom. Aber bereits in endlichdimensionalen Räumen über endlichen Körpern ergeben sich interessante Fragen: Wieviele Basen hat ein solcher Vektorraum? Wie gross ist die Wahrscheinlichkeit eine Basis zu finden, wenn man eine zufällige Kollektion von Vektoren herausgreift? Wie verhält sich diese Wahrscheinlichkeit, wenn die Dimension oder die Kardinalität des Körpers gross wird? Bei der Beantwortung dieser Fragen spielen zahlentheoretische Erwägungen eine Rolle, aber auch der Eulersche Pentagonalzahlensatz und die Theorie elliptischer Funktionen tauchen an überraschender Stelle auf. Der Autor der vorliegenden Arbeit illustriert seine Ausführungen mit numerischen Daten.

In the vector space V, we set out to find a basis at random. How effective is this method? On average, how many trials are needed to succeed? What happens as q increases? As n increases? How many distinct bases does V have? We answer these and other related questions, and we provide numerical results that illustrate the method's performance. Intriguingly, we were led to consider and apply the Jacobi theta functions from complex analysis. Also, we discuss a couple of number-theoretic results that are related to the method's success-probability limit as $n \to \infty$, for fixed q, that is, $\lim_{q \in \mathcal{Q}; n \to \infty} P_{n,q}(\text{success})$.

The tabulated numerical data were obtained with Maple 18.02, setting the environment variable `Digits := 15`. The output data were rounded to the number of decimal places shown in the tables.

We collect and summarize our results in Section 6.

Although the motivating problems are different, our work intersects that of Brennan and Wolfskill [5] and Waterhouse [10]. We mention differences and similarities as they occur.

Similar problems have been considered since long ago. For example, in 1893, Landsberg [9] determined the number of matrices – rectangular or square – that have a given rank, modulo a fixed prime. About one hundred years later, Gerth [6] investigated more general, related questions.

Among the novel and salient features of the paper, we have the following.

- In terms of just one Jacobi theta function, we provide an attainable, optimal lower bound for the sequence $\left(\lim_{n \to \infty} P_{n,q}\,(\text{success})\right)_{q \in \mathcal{Q}}$, whose limit as $q \to \infty$ is the said optimal lower bound.
- We discuss and present explicit expressions for the expected value and the variance for the number of trials until, and including, the trial when a basis is obtained. We give expressions for the limits, both when $q \to \infty$ and when $n \to \infty$.
- We present extensive numerical data that illustrate the behavior toward the various limits we discuss.
- In general, our exposition is detailed. This applies, in particular, to the Jacobi theta functions, to the connections with number theory, and to the references.

2 Success Probability

Under the discrete uniform probability law, we sample one element $\{v_1, \ldots, v_n\}$ from the set $\mathcal{S}$ of n-element subsets of V. The selected subset is a basis for V if and only if $v_1, \ldots, v_n$ are linearly independent, which occurs if and only if $v_1 \neq 0$ and, for each $j = 2, \ldots, n$, the vector $v_j \notin \text{Span}\left(\left\{v_1, \ldots, v_{j-1}\right\}\right)$. Thus, for $v_1, \ldots, v_n$ to be linearly independent, there are $q^n - 1$ choices for v_1 and, for each $j = 2, \ldots, n$, there are $q^n - q^{j-1}$ choices for v_j. Therefore, there are

$$(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$$

such linearly independent sets $\{v_1, \ldots, v_n\}$ in $\mathcal{S}$; also, that is the number of distinct bases in V. Consequently, the success probability $P_{n,q}(\text{success})$ – the probability that $\{v_1, \ldots, v_n\}$

is a basis for V – is

$$\begin{aligned} P_{n,q}(\text{success}) &= (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})/q^{n^2} \\ &= (1-q^{-1})(1-q^{-2})\cdots(1-q^{-n}). \end{aligned}$$

The preceding argument is essentially the same as that given in [10] to determine the probability that the determinant of a random $n \times n$ matrix over $\mathbb{F}_q$ is not zero. We present the argument here for completeness.

3 Success Probability as $q \to \infty$

For fixed n, it is reasonable to think that, for $q \in \mathcal{Q}$ and as $q \to \infty$, linear dependencies should be less and less likely in a random set of n vectors, and, therefore, the success probability should increase. Indeed, for a fixed integer $n > 0$, and for each positive integer r, let

$$\alpha_r(n) := (1-r^{-1})(1-r^{-2})\cdots(1-r^{-n}).$$

Then, as $r \to \infty$, the sequence $(\alpha_r(n))_{r=1}^{\infty}$ converges because it is strictly monotone increasing and bounded above by one. In fact, $\lim_{r\to\infty}\alpha_r(n) = 1$. Therefore, the subsequence $\mathcal{Q}$ has the same limit; that is,

$$\lim_{q\in\mathcal{Q};q\to\infty} P_{n,q}(\text{success}) = \lim_{q\in\mathcal{Q};q\to\infty}(1-q^{-1})(1-q^{-2})\cdots(1-q^{-n}) = 1.$$

For fixed n, and as $q \to \infty$, the data in Tables 1 through 3 illustrate how $P_{n,q}(\text{success})$ increases to its limit value of 1. For example, when $n = 10$, already $P_{n,q}(\text{success} \mid q = 2^6) \approx 0.98$, and then $P_{n,q}(\text{success} \mid q = 5^6) \approx 0.999936$.

Table 1: The success probability $\prod_{k=1}^{n}(1-q^{-k})$ when $q = 2, 2^3$, and 2^6, for increasing values of n

n	$q = 2$	$q = 2^3$	$q = 2^6$
10	0.289070298	0.859405995	0.984130860
100	0.288788095	0.859405994	0.984130860
500	0.288788095	0.859405994	0.984130860
∞ (limit value)	0.288787934	0.859405994	0.984130860

Table 2: The success probability $\prod_{k=1}^{n}(1-q^{-k})$ when $q = 3, 3^3$, and 3^6, for increasing values of n

n	$q = 3$	$q = 3^3$	$q = 3^6$
10	0.560130821	0.961591291	0.998626376
100	0.560126078	0.961591291	0.998626376
500	0.560126078	0.961591291	0.998626376
∞ (limit value)	0.560126078	0.961591291	0.998626376

Table 3: The success probability $\prod_{k=1}^{n}(1-q^{-k})$ when $q=5, 5^3$, and 5^6, for increasing values of n

n	$q=5$	$q=5^3$	$q=5^6$
10	0.760332815	0.991936000	0.999935996
100	0.760332796	0.991936000	0.999935996
500	0.760332796	0.991936000	0.999935996
∞ (limit value)	0.760332796	0.991936000	0.999935996

4 Success Probability as $n \to \infty$

Intuitively, for fixed $q \in \mathcal{Q}$ and as $n \to \infty$, linear dependencies should be more and more likely in a random set of n vectors, and, therefore, the success probability should decrease. Indeed, for a fixed integer $r > 1$, and for each positive integer n, let

$$\beta_n(r) := (1-r^{-1})(1-r^{-2})\cdots(1-r^{-n}).$$

Then, as $n \to \infty$, the sequence $(\beta_n(r))_{n=1}^{\infty}$ converges because it is strictly monotone decreasing and bounded below by zero. Thus, for each $q \in \mathcal{Q}$,

$$\lim_{q\in\mathcal{Q};n\to\infty} P_{n,q}(\text{success}) = \lim_{q\in\mathcal{Q};n\to\infty} (1-q^{-1})(1-q^{-2})\cdots(1-q^{-n}) \tag{1}$$

exists, but it is not equal to zero, as one might be tempted to think; in fact, that limit value is always greater than 0.2887, as shown in Section 4.2. The limit in (1) can be determined through old, venerable functions that we discuss next.

4.1 The Jacobi theta functions

Part of elliptic-function theory, the four Jacobi theta functions ϑ_1, ϑ_2, ϑ_3, and ϑ_4 are functions of a complex variable z, and they also depend on a constant parameter s. Instead of s, the usual notation for the parameter is q; however, we have already reserved q for the cardinality of a finite field.

Let the variable $z \in \mathbb{C}$, and let the constant parameter $s := e^{\pi i \tau}$, where the imaginary part $\text{Im}(\tau) > 0$, so that $|s| < 1$. The definitions ([8, p. 156] and [11, pp. 463–464]) are as follows:

$$\vartheta_1(z,s) := 2\sum_{k=0}^{\infty}(-1)^k s^{\frac{1}{4}(2k+1)^2}\sin\{(2k+1)z\},$$

$$\vartheta_2(z,s) := 2\sum_{k=0}^{\infty} s^{\frac{1}{4}(2k+1)^2}\cos\{(2k+1)z\},$$

$$\vartheta_3(z,s) := 1+2\sum_{k=1}^{\infty} s^{k^2}\cos(2kz),$$

and

$$\vartheta_4(z,s) := 1 + 2\sum_{k=1}^{\infty}(-1)^k s^{k^2}\cos(2kz).$$

All of these series converge very fast [8, p. 157]; this is illustrated by our tabulated numerical data. For a fixed constant s, the four Jacobi theta functions are entire functions of z.

The notation ϑ is sometimes used for ϑ_4 [11, pp. 463–464].

It is clear that $\vartheta_1(0,s) = 0$. When $z = 0$, and the value of the constant parameter s is understood, it is customary to omit the arguments, and simply write

$$\begin{aligned} &\vartheta_j(0,s) =: \vartheta_j \text{ for } j = 2,3,4, \qquad \text{and} \\ &\vartheta_1'(0,s) =: \vartheta_1' \end{aligned}$$

for the derivative of $\vartheta_1(z,s)$ with respect to z, at $z = 0$.

When $z = 0$, the four theta functions are related by the following equation ([8, p. 166] and [11, p. 470]):

$$\vartheta_1'(0,s) = \vartheta_2(0,s)\vartheta_3(0,s)\vartheta_4(0,s). \tag{2}$$

The Jacobi theta functions have product representations, as follows ([8, p. 163] and [11, Sections 21.3 and 21.42, pp. 469–470, 472–473]):

$$\begin{aligned}
\vartheta_1(z,s) &= 2\left\{\prod_{k=1}^{\infty}(1-s^{2k})\right\} s^{\frac{1}{4}}\sin(z)\prod_{k=1}^{\infty}\{1-2s^{2k}\cos(2z)+s^{4k}\}, \\
\vartheta_2(z,s) &= 2\left\{\prod_{k=1}^{\infty}(1-s^{2k})\right\} s^{\frac{1}{4}}\cos(z)\prod_{k=1}^{\infty}\{1+2s^{2k}\cos(2z)+s^{4k}\}, \\
\vartheta_3(z,s) &= \left\{\prod_{k=1}^{\infty}(1-s^{2k})\right\}\prod_{k=1}^{\infty}\{1+2s^{2k-1}\cos(2z)+s^{4k-2}\}, \qquad \text{and} \\
\vartheta_4(z,s) &= \left\{\prod_{k=1}^{\infty}(1-s^{2k})\right\}\prod_{k=1}^{\infty}\{1-2s^{2k-1}\cos(2z)+s^{4k-2}\}.
\end{aligned} \tag{3}$$

Each of the product representations in (3) contains $\prod_{k=1}^{\infty}(1-s^{2k})$ as a factor; this suggests that these theta functions may be used to determine the limit $\prod_{k=1}^{\infty}\left(1-q^{-k}\right)$ that we are interested in.

4.2 The value of $\lim_{q\in\mathcal{Q};n\to\infty}(1-q^{-1})(1-q^{-2})\cdots(1-q^{-n})$

Our departure point is the fact that ([8, Equation (13.5.32), p. 165] and [11, pp. 472–473])

$$\vartheta_1'(0,s) = 2s^{\frac{1}{4}}\left\{\prod_{k=1}^{\infty}(1-s^{2k})\right\}\left\{\prod_{k=1}^{\infty}(1-s^{2k})^2\right\} = 2s^{\frac{1}{4}}\left\{\prod_{k=1}^{\infty}(1-s^{2k})\right\}^3, \tag{4}$$

since the products converge absolutely. In (4) we replace s by $q^{-1/2}$, and then

$$\vartheta_1'(0, q^{-1/2}) = 2\left(q^{-1/2}\right)^{\frac{1}{4}}\left[\prod_{k=1}^{\infty}\left\{1-\left(q^{-1/2}\right)^{2k}\right\}\right]^3 = 2q^{-1/8}\left\{\prod_{k=1}^{\infty}\left(1-q^{-k}\right)\right\}^3.$$

Therefore, we can now obtain the value of the desired limit:

$$\prod_{k=1}^{\infty}\left(1-q^{-k}\right) = \left\{\frac{1}{2}q^{1/8}\vartheta_1'\left(0, q^{-1/2}\right)\right\}^{1/3} = q^{\frac{1}{24}}\left\{\frac{1}{2}\vartheta_1'\left(0, q^{-1/2}\right)\right\}^{1/3}, \quad (5)$$

simpler than the expression given in [5, Theorem 4, p. 313], which involves three of the theta functions. Another, more complicated, expression for the desired limit follows by applying the result in Equations (2) to (5). Doing so, we find

$$\prod_{k=1}^{\infty}\left(1-q^{-k}\right) = q^{\frac{1}{24}}\left\{\frac{1}{2}\vartheta_2\left(0, q^{-1/2}\right)\vartheta_3\left(0, q^{-1/2}\right)\vartheta_4\left(0, q^{-1/2}\right)\right\}^{1/3},$$

which, however, does not appear to be the same as that given in [5, Theorem 4, p. 313], taking into account that, as we have mentioned earlier, sometimes the notation ϑ is used for ϑ_4. Nevertheless, our numerical data agree with the corresponding data in [5], always to at least five decimal places.

For fixed $q \in \mathcal{Q}$, and as $n \to \infty$, the data in Tables 1 through 3 illustrate the manner in which $P_{n,q}$(success) decreases to its limit value. For example, when $q = 2$, already $P_{n,q}(\text{success} \mid n = 10) \approx 0.289070$, and, in this case, the limit value $\lim_{q\in\mathcal{Q};n\to\infty} P_{n,q}$ (success) ≈ 0.28878793. For larger values of q, we see in these tables that the convergence is faster.

4.3 Attainable, optimal lower bound for the sequence $\left(\lim_{n\to\infty}\prod_{k=1}^{n}\left(1-q^{-k}\right)\right)_{q\in\mathcal{Q}}$

Brennan and Wolfskill [5, Theorem 2, p. 312] state that, for $q \in \mathcal{Q}$,

$$\lim_{n\to\infty}\prod_{k=1}^{n}(1-q^{-k}) \geq \frac{2}{9}.$$

Following a referee's question, we present an outline of Brennan and Wolfskill's argument. Let $q \in \mathcal{Q}$. They begin by showing that

$$\prod_{k=1}^{\infty}(1-q^{-k}) \geq \frac{q-2}{q-1}.$$

This is achieved by first using induction on n to obtain the inequality

$$\prod_{k=1}^{n}(1-q^{-k}) \geq 1-\sum_{k=1}^{n}q^{-k},$$

and then taking limits as $n \to \infty$ and summing the geometric series $\sum_{k=1}^{\infty} q^{-k}$. They then state that

$$\prod_{k=1}^{\infty}(1-q^{-k}) \geq (1-q^{-1})\prod_{k=1}^{\infty}(1-q^{2k})^2 = (1-q^{-1})\left[\prod_{k=1}^{\infty}\left\{1-\left(q^2\right)^{-k}\right\}\right]^2. \qquad (6)$$

Finally, the conclusion is obtained by using the previous lower bound $(q-2)/(q-1)$ and the fact that the sequence $\left(\lim_{n\to\infty}\prod_{k=1}^{n}\left(1-q^{-k}\right)\right)_{q\in\mathcal{Q}}$ is monotonically increasing. Thus, when $q := 2$, from (6),

$$\prod_{k=1}^{\infty}(1-2^{-k}) \geq \frac{1}{2}\left\{\prod_{k=1}^{\infty}\left(1-4^{-k}\right)\right\}^2 \geq \frac{1}{2}\left(\frac{2}{3}\right)^2 = \frac{2}{9}.$$

The lower bound $2/9$ can be improved to produce an attainable, optimal lower bound in terms of just one Jacobi theta function, as follows.

We have seen that, for a fixed positive integer n, and for each positive integer r, if

$$\alpha_r(n) := (1-r^{-1})(1-r^{-2})\cdots(1-r^{-n}),$$

then the sequence $(\alpha_r\,(n))_{r=1}^{\infty}$ is strictly monotone increasing. Thus, for a fixed positive integer n, and for each integer $r > 2$,

$$(1-2^{-1})(1-2^{-2})\cdots(1-2^{-n}) < (1-r^{-1})(1-r^{-2})\cdots(1-r^{-n}). \qquad (7)$$

We have also seen that, for a fixed $q \in \mathcal{Q}$, and for each positive integer n, from (5),

$$\lim_{q\in\mathcal{Q};n\to\infty}(1-q^{-1})(1-q^{-2})\cdots(1-q^{-n}) = q^{\frac{1}{24}}\left\{\frac{1}{2}\vartheta_1'\left(0,q^{-1/2}\right)\right\}^{1/3}. \qquad (8)$$

Therefore, from (7) and (8), we have, for each $q \in \mathcal{Q}$,

$$\lim_{n\to\infty}(1-2^{-1})(1-2^{-2})\cdots(1-2^{-n}) \leq \lim_{q\in\mathcal{Q};n\to\infty}(1-q^{-1})(1-q^{-2})\cdots(1-q^{-n})$$

and, from Table 1,

$$0.2887 < 2^{\frac{1}{24}}\left\{\frac{1}{2}\vartheta_1'\left(0,2^{-1/2}\right)\right\}^{1/3} \leq q^{\frac{1}{24}}\left\{\frac{1}{2}\vartheta_1'\left(0,q^{-1/2}\right)\right\}^{1/3}. \qquad (9)$$

In (9), the lower bound

$$2^{\frac{1}{24}}\left\{\frac{1}{2}\vartheta_1'\left(0,2^{-1/2}\right)\right\}^{1/3}$$

is best possible for the sequence

$$\left(\lim_{n\to\infty}\prod_{k=1}^{n}\left(1-q^{-k}\right)\right)_{q\in\mathcal{Q}},$$

and it is attained if and only if $q = 2$.

4.4 Connections with number theory

The infinite product $\prod_{n=1}^{\infty}\left(1-q^{-n}\right)=\lim_{q\in\mathcal{Q};n\to\infty}P_{n,q}(\text{success})$ is connected to number theory, via the pentagonal numbers and the partition function. These connections lead to additional expressions – infinite power series – for the product $\prod_{n=1}^{\infty}\left(1-q^{-n}\right)$. Convergence of these series is not necessarily an issue in number theory, where such series are often treated as formal expressions. However, we are interested in the limit values, and that is why we have stated convergence conditions on x in the theorems in this section.

The first connection ([2, Theorem 14–4, pp. 176–177], [3, Theorem 14.3, p. 312], and [4, Theorem 1.2, p. 139]) goes back to Euler.

Theorem 1 (**Euler's pentagonal-number theorem**). *To ensure convergence, we let x be a complex variable with $|x|<1$. Then*

$$\prod_{k=1}^{\infty}\left(1-x^k\right)=1-x-x^2+x^5+x^7-x^{12}-x^{15}+\cdots$$
$$=1+\sum_{k=1}^{\infty}(-1)^k\left\{x^{(3k^2-k)/2}+x^{(3k^2+k)/2}\right\}=\sum_{k=-\infty}^{\infty}(-1)^k x^{(3k^2-k)/2}.\quad\square$$

Substituting q^{-1} for x in Euler's pentagonal-number theorem, we have, for each $q\in\mathcal{Q}$,

$$\begin{aligned}\lim_{q\in\mathcal{Q};n\to\infty}P_{n,q}(\text{success})&=\prod_{n=1}^{\infty}\left(1-q^{-n}\right)\\&=1-q^{-1}-q^{-2}+q^{-5}+q^{-7}-q^{-12}-q^{-15}+\cdots\\&=1+\sum_{k=1}^{\infty}(-1)^k\left\{q^{-(3k^2-k)/2}+q^{-(3k^2+k)/2}\right\}\\&=\sum_{k=-\infty}^{\infty}(-1)^k q^{-(3k^2-k)/2}.\end{aligned}$$

Euler's theorem is called *pentagonal* because the (*generalized*) *pentagonal numbers* $\left(k\left(3k\pm1\right)/2\right)_{k=1}^{\infty}$ are related to pentagonal arrangements of points on the plane; see, e.g., [1, p. 16] and [7, p. 224].

For the second connection, we recall that a *partition* of a positive integer k is a multiset of positive integers whose sum is equal to k. The value $p(k)$ of the *partition function* $p(\cdot)$ is the number of distinct partitions of k. It is convenient to set $p(0):=1$. The next result is well known; see, for example, [3, Theorem 14.2, p. 308], [4, Corollary 1, p. 139], and [7, p. 223].

Theorem 2 (**Generating function for partitions**). *To ensure convergence, we let x be a complex variable with $|x|<1$. Then the generating function F for partitions*

$$F(x)=\sum_{k=0}^{\infty}p(k)x^k=\prod_{k=1}^{\infty}\frac{1}{1-x^k}=\frac{1}{(1-x)(1-x^2)(1-x^3)\cdots}.\quad\square$$

We can now relate $\lim_{q\in\mathcal{Q};n\to\infty} P_{n,q}(\text{success})$ to partitions, as follows. Substituting q^{-1} for x in Theorem 2, it follows that

$$\lim_{q\in\mathcal{Q};n\to\infty} P_{n,q}(\text{success}) = \prod_{n=1}^{\infty}\left(1-q^{-n}\right) = 1\Big/\sum_{k=0}^{\infty} p(k)q^{-k}.$$

Brennan and Wolfskill [5] and Waterhouse [10] use Euler's pentagonal-number theorem to express $\prod_{n=1}^{\infty}\left(1-q^{-n}\right)$ as an infinite series. Waterhouse [10] mentions partitions, but does not say what the limit value of $\prod_{n=1}^{\infty}\left(1-q^{-n}\right)$ is actually equal to.

The referee noted that Euler's pentagonal-number theorem is used to prove the Jacobi triple-product identity and asked whether that theorem is used to prove (2). In their discussion of Jacobi theta functions, the references [8, 11] do not mention Euler's pentagonal-number theorem or the Jacobi triple-product identity. The pentagonal-number theorem is itself a special case of the triple-product identity [7, p. 226]. Next, for completeness, we state two forms of the triple-product identity [4, Problem 28, p. 195] and [7, Theorem 8, p. 226].

Theorem 3 (**Jacobi triple-product identity**). *If x and y are complex numbers such that $|x| < 1$ and $y \neq 0$, then*

- $\prod_{k=1}^{\infty}(1-x^{2k})(1+x^{2k-1}y)(1+x^{2k-1}y^{-1}) = \sum_{k=-\infty}^{\infty} x^{k^2}y^k$ *and*
- $\prod_{k=1}^{\infty}(1-x^{2k})(1-x^{2k-1}y^2)(1-x^{2k-1}y^{-2}) = \sum_{k=-\infty}^{\infty}(-1)^k x^{k^2}y^{2k}$. □

One form of the Jacobi theta function $\vartheta_4(z,s)$ lends itself well to the application of the triple-product identity. Let $|s| < 1$. The Jacobi theta function $\vartheta_4(z,s)$ can be written [11, p. 463]

$$\vartheta_4(z,s) = \sum_{k=-\infty}^{\infty}(-1)^k s^{k^2} e^{2kiz}. \tag{10}$$

Thus, it is clear that, by taking $x := s$ and $y := e^{iz}$, we can apply the second form of the Jacobi triple-product identity in Theorem 3 to the series in (10) to obtain

$$\vartheta_4(z,s) = \prod_{k=1}^{\infty}(1-s^{2k})(1-s^{2k-1}e^{2iz})(1-s^{2k-1}e^{-2iz}). \tag{11}$$

Moreover, using Euler's formula $e^{iw} = \cos(w) + i\sin(w)$ and basic trigonometric identities, it is straightforward to show that

$$(1-s^{2k-1}e^{2iz})(1-s^{2k-1}e^{-2iz}) = 1 - 2s^{2k-1}\cos(2z) + s^{4k-2},$$

and so (11) becomes

$$\vartheta_4(z,s) = \prod_{k=1}^{\infty}(1-s^{2k})(1-2s^{2k-1}\cos(2z)+s^{4k-2}),$$

the expression given earlier in (3) for $\vartheta_4(z,s)$. Thus, we see a connection between the tools we use and the Jacobi triple-product identity.

5 How Many Trials?

Under the discrete uniform probability law, and drawing one item at a time, we sample with replacement from $\mathcal{S}$ until we obtain a basis for V. If T is the number of samples taken until, and including, the trial when we obtain a basis, then T is a geometric random variable with support $\{1, 2, 3, \ldots\}$ and parameter – the constant success probability – equal to

$$(1 - q^{-1})(1 - q^{-2}) \cdots (1 - q^{-n}) =: \psi_{n,q}.$$

The probability law for T is

$$P(T = t) = \psi_{n,q}(1 - \psi_{n,q})^{t-1}, \quad t = 1, 2, 3, \ldots;$$

the expected value $E[T] = 1/\psi_{n,q}$; and the variance $\mathrm{Var}[T] = (1 - \psi_{n,q})/\psi_{n,q}^2$. For fixed n and q, small values simultaneously for both $E[T]$ and $\mathrm{Var}[T]$ suggest that a basis is likely to be found after just a few trials.

5.1 Expected value and variance as $q \to \infty$

From Sections 3 and 5, it is clear that, for fixed n,

$$\lim_{q \in \mathcal{Q}; q \to \infty} E[T] = 1 \quad \text{and} \quad \lim_{q \in \mathcal{Q}; q \to \infty} \mathrm{Var}[T] = 0.$$

These limit values make sense. Intuitively, for fixed n, and as $q \to \infty$, dependencies between vectors should be less and less likely, so for large q we would expect to draw a basis very quickly. The data in Tables 4 through 6 support this conclusion.

Table 4: Cumulative probability of obtaining a basis on or before the tth trial, and the expected value $E[T]$, for $q = 2, 2^3$, and 2^6, and some values of n

	$q = 2$			$q = 2^3$			$q = 2^6$		
t	$n = 2$	$n = 4$	$n = 10$	$n = 2$	$n = 4$	$n = 10$	$n = 2$	$n = 4$	$n = 10$
1	0.3750	0.3076	0.2891	0.8613	0.8594	0.8594	0.9841	0.9841	0.9841
2	0.6094	0.5206	0.4946	0.9808	0.9802	0.9802	0.9997	0.9997	0.9997
3	0.7559	0.6681	0.6407	0.9973	0.9972	0.9972	1.0000	1.0000	1.0000
4	0.8474	0.7702	0.7445	0.9996	0.9996	0.9996	1.0000	1.0000	1.0000
5	0.9046	0.8409	0.8184	0.9999	0.9999	0.9999	1.0000	1.0000	1.0000
6	0.9404	0.8898	0.8709	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
7	0.9627	0.9237	0.9082	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
8	0.9767	0.9472	0.9347	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
9	0.9854	0.9634	0.9536	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
10	0.9909	0.9747	0.9670	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
$E[T]$	2.67	3.25	3.46	1.16	1.16	1.16	1.02	1.02	1.02

For fixed n, and as $q \to \infty$, the data in Tables 7 through 9 illustrate the manner in which $E[T]$ and $\mathrm{Var}[T]$ approach their limit values. For example, when $n = 10$, $E[T \mid q = 2] \approx 3.46$ and $E[T \mid q = 5] \approx 1.32$, and $\mathrm{Var}[T \mid q = 2] \approx 8.51$ and $\mathrm{Var}[T \mid q = 5] \approx 0.42$.

Table 5: Cumulative probability of obtaining a basis on or before the tth trial, and the expected value $E[T]$, for $q = 3, 3^3$, and 3^6, and some values of n

	$q = 3$			$q = 3^3$			$q = 3^6$		
t	$n = 2$	$n = 4$	$n = 10$	$n = 2$	$n = 4$	$n = 10$	$n = 2$	$n = 4$	$n = 10$
1	0.5926	0.5636	0.5601	0.9616	0.9616	0.9616	0.9986	0.9986	0.9986
2	0.8340	0.8096	0.8065	0.9985	0.9985	0.9985	1.0000	1.0000	1.0000
3	0.9324	0.9169	0.9149	0.9999	0.9999	0.9999	1.0000	1.0000	1.0000
4	0.9725	0.9637	0.9626	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
5	0.9888	0.9842	0.9835	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
6	0.9954	0.9931	0.9928	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
7	0.9981	0.9970	0.9968	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
8	0.9992	0.9987	0.9986	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
9	0.9997	0.9994	0.9994	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
10	0.9999	0.9997	0.9997	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
$E[T]$	1.69	1.77	1.79	1.04	1.04	1.04	1.00	1.00	1.00

Table 6: Cumulative probability of obtaining a basis on or before the tth trial, and the expected value $E[T]$, for $q = 5, 5^3$, and 5^6, and some values of n

	$q = 5$			$q = 5^3$			$q = 5^6$		
t	$n = 2$	$n = 4$	$n = 10$	$n = 2$	$n = 4$	$n = 10$	$n = 2$	$n = 4$	$n = 10$
1	0.7680	0.7606	0.7603	0.9919	0.9919	0.9919	0.9999	0.9999	0.9999
2	0.9462	0.9427	0.9426	0.9999	0.9999	0.9999	1.0000	1.0000	1.0000
3	0.9875	0.9863	0.9862	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
4	0.9971	0.9967	0.9967	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
5	0.9993	0.9992	0.9992	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
6	0.9998	0.9998	0.9998	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
7	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
8	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
9	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
10	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
$E[T]$	1.30	1.31	1.32	1.01	1.01	1.01	1.00	1.00	1.00

5.2 Expected value and variance as $n \to \infty$

From Sections 4.2, 4.4, and 5, it is clear that, for fixed $q \in \mathcal{Q}$,

$$\begin{aligned}\lim_{q\in\mathcal{Q};n\to\infty} E[T] &= q^{-1/24}\left\{\frac{1}{2}\vartheta_1'\left(0, q^{-1/2}\right)\right\}^{-1/3} = 1\Big/\sum_{k=-\infty}^{\infty}(-1)^k q^{-(3k^2-k)/2}\\ &= \sum_{k=0}^{\infty} p(k)q^{-k},\end{aligned}$$

and

$$\lim_{q\in\mathcal{Q};n\to\infty}\mathrm{Var}[T] = \left[q^{1/24}\left\{\frac{1}{2}\vartheta_1'\left(0, q^{-1/2}\right)\right\}^{1/3}\right]^{-2} - \left[q^{1/24}\left\{\frac{1}{2}\vartheta_1'\left(0, q^{-1/2}\right)\right\}^{1/3}\right]^{-1}$$

$$
\begin{aligned}
&= \left[\sum_{k=-\infty}^{\infty} (-1)^k q^{-(3k^2-k)/2} \right]^{-2} - \left[\sum_{k=-\infty}^{\infty} (-1)^k q^{-(3k^2-k)/2} \right]^{-1} \\
&= \left[\sum_{k=0}^{\infty} p(k) q^{-k} - 1 \right] \left[\sum_{k=0}^{\infty} p(k) q^{-k} \right].
\end{aligned}
$$

For fixed $q \in \mathcal{Q}$, and as $n \to \infty$, the data in Tables 7 through 9 show that for all tabulated values of q, both $E[T]$ and $\mathrm{Var}[T]$ already achieve their rounded limit values when $n = 10$.

Table 7: Expected value $E[T]$ and variance $\mathrm{Var}[T]$ when $q = 2, 2^3$, and 2^6, for increasing values of n

	$q=2$		$q=2^3$		$q=2^6$	
n	$E[T]$	$\mathrm{Var}[T]$	$E[T]$	$\mathrm{Var}[T]$	$E[T]$	$\mathrm{Var}[T]$
10	3.46	8.51	1.16	0.19	1.02	0.02
100	3.46	8.53	1.16	0.19	1.02	0.02
500	3.46	8.53	1.16	0.19	1.02	0.02
∞ (limit value)	3.46	8.53	1.16	0.19	1.02	0.02

Table 8: Expected value $E[T]$ and variance $\mathrm{Var}[T]$ when $q = 3, 3^3$, and 3^6, for increasing values of n

	$q=3$		$q=3^3$		$q=3^6$	
n	$E[T]$	$\mathrm{Var}[T]$	$E[T]$	$\mathrm{Var}[T]$	$E[T]$	$\mathrm{Var}[T]$
10	1.79	1.402	1.04	0.042	1.00	0.001
100	1.79	1.402	1.04	0.042	1.00	0.001
500	1.79	1.402	1.04	0.042	1.00	0.001
∞ (limit value)	1.79	1.402	1.04	0.042	1.00	0.001

Table 9: Expected value $E[T]$ and variance $\mathrm{Var}[T]$ when $q = 5, 5^3$, and 5^6, for increasing values of n

	$q=5$		$q=5^3$		$q=5^6$	
n	$E[T]$	$\mathrm{Var}[T]$	$E[T]$	$\mathrm{Var}[T]$	$E[T]$	$\mathrm{Var}[T]$
10	1.32	0.415	1.01	0.008	1.00	0.00006
100	1.32	0.415	1.01	0.008	1.00	0.00006
500	1.32	0.415	1.01	0.008	1.00	0.00006
∞ (limit value)	1.32	0.415	1.01	0.008	1.00	0.00006

6 Summary and Conclusion

Next, we collect and summarize our results.

Theorem 4. *Let $\mathcal{Q} := (2, 3, 2^2, 5, 7, 2^3, 3^2, \ldots)$, the sequence of prime powers, and let $q \in \mathcal{Q}$. Over the finite field $\mathbb{F}_q$ of q elements, let V be a vector space of finite dimension n. Let $\mathcal{S}$ be the set of n-element subsets of V. Under the discrete uniform probability law, and* *drawing one item at a time, we sample with replacement from $\mathcal{S}$ until we obtain a basis for V. Let $P_{n,q}(\text{success})$ denote the success probability. Then the following conclusions are valid.*

- *There are $(q^n - 1)(q^n - q)(q^n - q^2)\cdots(q^n - q^{n-1})$ distinct bases in V.*
- *For each individual draw, the probability of obtaining a basis is equal to $P_{n,q}(\text{success}) = (1 - q^{-1})(1 - q^{-2})\cdots(1 - q^{-n})$.*
  - *For fixed n,* $\lim\limits_{q\in\mathcal{Q};q\to\infty} P_{n,q}(\text{success}) = \lim\limits_{q\in\mathcal{Q};q\to\infty}(1 - q^{-1})(1 - q^{-2})\cdots(1 - q^{-n}) = 1.$
  - *For fixed $q \in \mathcal{Q}$,*

$$\begin{aligned}\lim_{q\in\mathcal{Q};n\to\infty} P_{n,q}(\text{success}) &= \lim_{q\in\mathcal{Q};n\to\infty}(1 - q^{-1})(1 - q^{-2})\cdots(1 - q^{-n})\\ &= q^{\frac{1}{24}}\left\{\frac{1}{2}\vartheta_1'\left(0, q^{-1/2}\right)\right\}^{1/3}\\ &= q^{\frac{1}{24}}\left\{\frac{1}{2}\vartheta_2\left(0, q^{-1/2}\right)\vartheta_3\left(0, q^{-1/2}\right)\vartheta_4\left(0, q^{-1/2}\right)\right\}^{1/3},\end{aligned}$$

    where $\vartheta_1, \vartheta_2, \vartheta_3,$ and ϑ_4 are the Jacobi theta functions.
  - *The sequence*

$$\left(\lim_{n\to\infty} P_{n,q}\ (\text{success})\right)_{q\in\mathcal{Q}} = \left(\lim_{n\to\infty}\prod_{k=1}^{n}\left(1 - q^{-k}\right)\right)_{q\in\mathcal{Q}}$$

    is monotonically increasing. For each $q \in \mathcal{Q}$,

$$0.2887 < 2^{\frac{1}{24}}\left\{\frac{1}{2}\vartheta_1'\left(0, 2^{-1/2}\right)\right\}^{1/3} \le q^{\frac{1}{24}}\left\{\frac{1}{2}\vartheta_1'\left(0, q^{-1/2}\right)\right\}^{1/3}.$$

    Best possible for the sequence

$$\left(\lim_{n\to\infty} P_{n,q}\ (\text{success})\right)_{q\in\mathcal{Q}} = \left(\lim_{n\to\infty}\prod_{k=1}^{n}\left(1 - q^{-k}\right)\right)_{q\in\mathcal{Q}},$$

    the lower bound

$$2^{\frac{1}{24}}\left\{\frac{1}{2}\vartheta_1'\left(0, 2^{-1/2}\right)\right\}^{1/3}$$

    is attained if and only if $q = 2$.
- *Let the random variable T be the number of trials – samples drawn – until, and including, the trial when we obtain a basis. Set*

$$(1 - q^{-1})(1 - q^{-2})\cdots(1 - q^{-n}) =: \psi_{n,q}.$$

  Then T is a geometric random variable with probability law $P(T = t) = \psi_{n,q}(1 - \psi_{n,q})^{t-1}$, $t = 1, 2, 3, \ldots$; expected value $E[T] = 1/\psi_{n,q}$; and variance $\mathrm{Var}[T] = (1 - \psi_{n,q})/\psi_{n,q}^2$.

- *For fixed n,* $\lim_{q\in\mathcal{Q};q\to\infty} E[T] = 1$ *and* $\lim_{q\in\mathcal{Q};q\to\infty} \operatorname{Var}[T] = 0$.
- *For fixed* $q \in \mathcal{Q}$,

$$\begin{aligned}\lim_{q\in\mathcal{Q};n\to\infty} E[T] &= q^{-1/24}\left\{\frac{1}{2}\vartheta_1'\left(0, q^{-1/2}\right)\right\}^{-1/3}\\ &= 1\bigg/\sum_{k=-\infty}^{\infty}(-1)^k q^{-(3k^2-k)/2}\\ &= \sum_{k=0}^{\infty} p(k)q^{-k},\end{aligned}$$

and

$$\begin{aligned}\lim_{q\in\mathcal{Q};n\to\infty} \operatorname{Var}[T] = {}&\left[q^{1/24}\left\{\frac{1}{2}\vartheta_1'\left(0, q^{-1/2}\right)\right\}^{1/3}\right]^{-2}\\ &-\left[q^{1/24}\left\{\frac{1}{2}\vartheta_1'\left(0, q^{-1/2}\right)\right\}^{1/3}\right]^{-1}\\ = {}&\left[\sum_{k=-\infty}^{\infty}(-1)^k q^{-(3k^2-k)/2}\right]^{-2} - \left[\sum_{k=-\infty}^{\infty}(-1)^k q^{-(3k^2-k)/2}\right]^{-1}\\ = {}&\left[\sum_{k=0}^{\infty} p(k)q^{-k} - 1\right]\left[\sum_{k=0}^{\infty} p(k)q^{-k}\right],\end{aligned}$$

where $p(\cdot)$ *is the number-theoretic partition function.* □

Of course, the preceding results can also be stated in terms of linear independence, rank, and other concepts related to a basis in linear algebra.

Our work shows that, in a finite-dimensional vector space over a finite field, finding bases at random is an efficient procedure, as we are likely to come up with a basis after just a few trials.

Acknowledgement. The author thanks a referee for constructive, thoughtful comments that helped improve the paper.

References

[1] Adams W.W., Goldstein L.J.: *Introduction to Number Theory*. Prentice-Hall, Englewood Cliffs, New Jersey, 1976.

[2] Andrews G.E.: *Number Theory*. Saunders, Philadelphia, 1971.

[3] Apostol T.M.: *Introduction to Analytic Number Theory*. Springer-Verlag, New York, 1976.

[4] Ayoub R.: *An Introduction to the Analytic Theory of Numbers*. American Mathematical Society, Providence, Rhode Island, 1963.

[5] Brennan J.P., Wolfskill J.: Remarks on the probability the determinant of an $n \times n$-matrix over a finite field vanishes. *Discrete Mathematics* 1987; 67: 311–313.

[6] Gerth F. III: Limit probabilities for coranks of matrices over GF(q). *Linear and Multilinear Algebra* 1986; 19: 79–93.

[7] Grosswald E.: *Topics from the Theory of Numbers*. Macmillan, New York, 1966.

[8] Hille E.: *Analytic Function Theory*, volume II, 2d ed. AMS Chelsea Publishing, American Mathematical Society, Providence, Rhode Island, 2002.

[9] Landsberg G.: Ueber eine Anzahlbestimmung und eine damit zusammenhängende Reihe. *Journal für die reine und angewandte Mathematik* 1893; 111: 87–88.

[10] Waterhouse W.C.: How often do determinants over finite fields vanish? *Discrete Mathematics* 1987; 65: 103–104.

[11] Whittaker E.T., Watson G.N.: *A Course of Modern Analysis*, 4th ed. Cambridge Univ Press, New York, 1962.

Osvaldo Marrero
Department of Mathematics and Statistics
Villanova University
800 Lancaster Avenue
Villanova, Pennsylvania 19085–1699, USA
e-mail: Osvaldo.Marrero@villanova.edu