CDMTCS Research Report Series

Linear Independence and Choice

Douglas Bridges
Department of Mathematics
University of Waikato

Fred Richman
Department of Mathematics
Florida Atlantic University

Peter Schuster
University of München

CDMTCS-037
May 1997

Centre for Discrete Mathematics and
Theoretical Computer Science

LINEAR INDEPENDENCE AND CHOICE

Douglas Bridges
University of Waikato

Fred Richman
Florida Atlantic University

Peter Schuster
University of München

30 April 1997

Abstract. The notions of linear and metric independence are investigated in relation to the property: if U is a set of $m+1$ independent vectors, and X is a set of m independent vectors, then adjoining some vector in U to X results in a set of $m+1$ independent vectors. A weak countable choice axiom is introduced, in the presence of which linear and metric independence are equivalent. Proofs are carried out in the context of intuitionistic logic.

1. Introduction

A commutative ring with identity is **local** if whenever $a+b$ is a unit, either a or b is a unit. A **Heyting field** is a commutative local ring such that if a is not a unit, then $a=0$. Any local ring has a natural inequality, $a \neq b$, defined to mean that $a-b$ is a unit. Because the ring is local, if $a+b \neq 0$, then $a \neq 0$ or $b \neq 0$, that is, the inequality is an apartness. In a Heyting field, this inequality is **tight**: if a is not different from b, then $a=b$. This does *not* mean that a Heyting field is **discrete**: that is, either $a \neq b$ or $a=b$.

A **Heyting vector space** is a module over a Heyting field, with an inequality such that the algebraic operations are strongly extensional—so that, for example, if $x+y \neq x'+y'$, then $x \neq x'$ or $y \neq y'$. In particular, if $x+y \neq 0$, then $x \neq 0$ or $y \neq 0$, and if $ax \neq 0$, then $a \neq 0$ and $x \neq 0$.

The complex numbers form a Heyting field. A normed vector space over the complex numbers, with $x \neq 0$ defined to be $\|x\| \neq 0$, is a Heyting vector space. As we will be dealing exclusively with Heyting fields and Heyting vector spaces, we will henceforth suppress the qualifier "Heyting."

Vectors $x_1, \ldots, x_n$ are **linearly independent** if $\sum a_i x_i \neq 0$ whenever some $a_i \neq 0$. Heyting called such a family "free" to distinguish this property from its contrapositive, weak linear independence: if $\sum a_i x_i = 0$, then $a_i = 0$ for all i. For normed vector spaces there is an even stronger form of independence: $x_1, \ldots, x_n$ are **metrically independent** if there exists $\delta > 0$ so that $\|\sum a_i x_i\| \geq \delta$ whenever $\sum |a_i| \geq 1$—or if, equivalently, the coordinate projections on the span of $x_1, \ldots, x_n$ are uniformly continuous. It is easily seen that metric independence implies linear independence.

Let Y be a subspace of a vector space, and x a vector. We say that x is in the **complement** of Y, and write $x \in Y^c$, if $x \neq y$ for each y in Y. Note that if $x \in Y^c$, then $ax + y \neq 0$ whenever $a \neq 0$ or $y \neq 0$. It is readily seen [4, Lemma XII.4.1] that $x_1, \ldots, x_n$ are linearly (metrically) independent if and only if x_i is in the complement of (bounded away from) the span of $x_1, \ldots, x_{i-1}$ for $i = 1, \ldots, n$.

An abstract vector space is **finite-dimensional** if it is spanned by a finite linearly independent family of vectors. For a normed space to be finite-dimensional, we require that it be spanned by a finite *metrically* independent family (see [1]). It is a question of what category we are operating in: vector spaces and strongly extensional linear transformations, or normed vector spaces and bounded linear transformations.

Heyting [3, Theorem 1, page 56] proved the following extension property for finite-dimensional vector spaces.

EXT. Let $u_1, \ldots, u_{m+1}$ and $x_1, \ldots, x_m$ be two families of linearly independent vectors. Then there exists i such that $x_1, \ldots, x_m, u_i$ is linearly independent.

The motivating problem for this paper was to establish EXT in a not necessarily finite-dimensional normed vector space. We prove the following results.

- EXT holds in normed vector spaces if "linearly independent" is replaced by "metrically independent", which is arguably the correct notion in a normed space (Theorem 5).
- Linear independence is the same as metric independence for strictly convex normed spaces (Corollary 8). These include Hilbert spaces and the L^p spaces for $1 < p < \infty$.
- Linear independence is the same as metric independence in an arbitrary normed space in the context of a weak countable choice principle that is classically true with no choice axiom. We show this by deriving from this principle a lemma of Bishop's that is used to prove that linear independence implies metric independence (Theorem 10).

Bishop [1, Lemma 7, page 177] showed that if Y is a nonempty, complete, located subset of a metric space, and $x \in Y^c$, then x is bounded away from Y. In fact, he constructed, for any point x, a point y_0 in Y such that if $x \neq y_0$, then $d(x, Y) > 0$. In the proof, Bishop tacitly uses countable choice, possibly even dependent choice.

The construction in the proof of Bishop's lemma suggests two properties that a subset Y might have:

1. Y is **strongly reflective**: for each x there exists y_0 in Y such that if $x \neq y_0$, then x is bounded away from Y.
2. Y is **reflective**: for each x there exists y_0 in Y such that if $x \neq y_0$, then $x \in Y^c$.

The first property makes sense in a metric space, the second in any set with an inequality.

We show that if every finite-dimensional subspace is reflective, then EXT holds (Corollary 4). This follows from a general theorem which is a positive form of the fact that an n-dimensional subspace cannot contain $n+1$ independent vectors (Theorem 3).

Note that a subset Y is reflective if it is the image of a strongly extensional retraction ρ. For in that case, $y_0 = \rho x$ has the property that if $x \neq y_0$, then $x \neq y$ for each y in Y. Indeed, either $x \neq y$ or $y_0 \neq y$; in the latter case, $\rho x \neq y = \rho y$ and so $x \neq y$.

2. Bishop's principle

Bishop's principle [1, Lemma 7, page 177] states that a nonempty, complete, located subset of a metric space is strongly reflective. Using the law of excluded middle, one can easily show that any nonempty closed subset of a metric space is strongly reflective: let $y_0 = x$ if x is in Y, and let y_0 be any element of Y otherwise. Bishop's principle has many applications, for example in the proof that an independent set of vectors in a normed vector space over a locally compact field is metrically independent (see [4, Theorem XII.4.2]).

Here is a proof of Bishop's principle using countable choice. The proof is not essentially different from Bishop's, but the appeal to countable choice is made explicit.

Theorem 1 [Bishop's principle]. *Any nonempty complete located subset of a metric space is strongly reflective.*

Proof. Let Y be a nonempty complete located subset, and x a point. We may assume that $d(x, Y) < 1$. Consider the sequence of nonempty sets

$$A_n = \{(1, y) : d(x, y) < 1/n\} \cup \{(0, 0) : d(x, Y) > 1/(n+1)\}.$$

Countable choice produces a sequence $a_n \in A_n$ such that if $a_n = (0, 0)$, then $a_{n+1} = (0, 0)$. From this construct a sequence in Y by replacing $(1, y)$ by y and $(0, 0)$ by y_n where $a_n = (1, y_n)$ and $a_{n+1} = (0, 0)$. This sequence converges to the required point y_0 in Y. □

In this proof we constructed a Cauchy sequence converging to y_0. To use sequential completeness, one often needs to invoke the full axiom of countable choice. However, if completeness is defined without appeal to sequences, then Bishop's principle can be established on the basis of a very weak countable axiom of choice—see Section 5.

In any vector space one can consider the property

($*$) each finite-dimensional subspace is reflective.

Using Bishop's principle, one can show that ($*$) holds for vector spaces over the real or complex numbers. As any summand Y is reflective (take y_0 to be the component of x in Y) finite-dimensional vector spaces satisfy ($*$) because EXT holds.

3. Systems of linear equations

In order to establish EXT, we are led to analyze systems of equations. The idea is that either the vectors $x_1, \ldots, x_m, u_i$ are independent, or there is a vector in the span of $x_1, \ldots, x_m$ that approximates u_i, in some sense. So either EXT holds, or there are $m+1$ vectors in an m-dimensional subspace that are close to independent vectors. To rule out this latter possibility, it would be helpful to be able show that the $m+1$ vectors were linearly dependent, that is, that a homogeneous system of linear equations, with more variables than equations, has a nontrivial solution.

This can't quite be done, constructively. A nontrivial solution to the equation $ax+by=0$, over the real numbers, would establish that either a divides b, or b divides a. But that property, for arbitrary real numbers a and b, is equivalent to Bishop's omniscience principle LLPO, so does not admit a constructive proof [6, Proposition 1.3]. We can, however, get approximate solutions that are uniformly nontrivial.

Theorem 2. *Let (a_{ij}) be an m-by-$m+1$ matrix over a valuated field, and δ a positive number. There exist $x_1, \ldots, x_{m+1}$ such that $\sum_{j=1}^{m+1} |x_j| \geq 1$ and $\sum_{i=1}^{m} \left|\sum_{j=1}^{m+1} a_{ij}x_j\right| < \delta$.*

Proof. When $m=0$, simply choose $x_1 = 1$. When $m > 0$, set $x_1 = 0$ and find a solution that works for the last $m-1$ rows. Either this solution works also for the first row, and we are done, or some $a_{1j} \neq 0$. We may assume that $a_{11} \neq 0$ and clear the first column with row operations to get a matrix (a'_{ij}) with $a'_{i1} = 0$ for $i > 1$, and $a'_{1j} = a_{1j}$ for all j. By induction we can find $x_2, \ldots, x_{m+1}$ such that $\sum_{j=2}^{m+1} |x_j| \geq 1$ and

$$\sum_{i=2}^{m} \left| \sum_{j=1}^{m+1} a'_{ij} x_j \right| < \delta.$$

Choose x_1 so that $\sum_{j=1}^{m+1} a_{1j}x_j = 0$. Reversing the row operations yields

$$\sum_{i=1}^{m} \left| \sum_{j=1}^{m+1} a_{ij} x_j \right| < \delta,$$

completing the proof. □

Here is a purely algebraic version of Theorem 2.

Theorem 3. *Let X be the linear span of $x_1, \ldots, x_n$ in a Heyting vector space. If $u_1, \ldots, u_{n+1}$ are linearly independent, and $\xi_1, \ldots, \xi_{n+1}$ are elements of X, then there exists i such that $u_i \neq \xi_i$.*

Proof. Either $\xi_1 \neq u_1$, in which case we are done, or else $\xi_1 \neq 0$. Suppose the latter; we will show, by induction, that $\xi_i \neq u_i$ for some i. Write

$$\xi_i = \sum_{j=1}^{n} a_{ij} x_j$$

for $i = 1, \ldots, n+1$. As $\xi_1 \neq 0$, we may assume that $a_{11} \neq 0$. For $i > 1$ let

$$\begin{aligned} \xi_i' &= \xi_i - (a_{i1}/a_{11})\xi_1, \\ u_i' &= u_i - (a_{i1}/a_{11})u_1. \end{aligned}$$

Then ξ_i' is in the span of $x_2, \ldots, x_n$, and $u_2', \ldots, u_{n+1}'$ are linearly independent. By induction, $\xi_i' \neq u_i'$ for some $i > 1$. It follows that either $\xi_i \neq u_i$ or $\xi_1 \neq u_1$. □

From Theorem 3 it follows that if finite-dimensional subspaces are reflective, then EXT holds.

Corollary 4. *Let $u_1, \ldots, u_{m+1}$ be linearly independent, and $x_1, \ldots, x_m$ vectors whose span X is reflective. Then there exists i such that $u_i \in X^c$. In particular, if $x_1, \ldots, x_m$ are linearly independent, then $x_1, \ldots, x_m, u_i$ is linearly independent.*

Proof. By reflectivity, there exist ξ_i in X such that if $u_i \neq \xi_i$, then $u_i \in X^c$. Theorem 3 says that $u_i \neq \xi_i$ for some i. □

We have the analogue of Corollary 4 for metric independence.

Theorem 5. *Let $u_1, \ldots, u_{m+1}$ be metrically independent, and $x_1, \ldots, x_m$ vectors whose linear span X is located. Then there exists i such that $d(u_i, X) > 0$. In particular, if $x_1, \ldots, x_m$ are metrically independent, then $x_1, \ldots, x_m, u_i$ are metrically independent.*

Proof. We may assume that $\|x_j\| \leq 1$. By metric independence, there is $\varepsilon > 0$ such that if $\sum |\lambda_i| \geq 1$, then $\sum \|\lambda_i u_i\| \geq \varepsilon$. Either the desired i exists, or $d(u_i, X) < \varepsilon/2(n+1)$ for all i. We will show that the latter leads to a contradiction.

If $d(u_i, X) < \varepsilon/2(n+1)$ for all i, then there exist a_{ji} such that

$$\left\| u_i - \sum_{j=1}^{n} a_{ji} x_j \right\| < \frac{\varepsilon}{2(n+1)}$$

for $i = 1, \ldots, n+1$. By Theorem 2, there exist $\lambda_1, \ldots, \lambda_{n+1}$ with $\sum |\lambda_i| = 1$ and

$$\sum_{j=1}^{n} \left| \sum_{i=1}^{n+1} a_{ji} \lambda_i \right| < \varepsilon/2.$$

So

$$\left\| \sum_{i=1}^{n+1} \lambda_i u_i - \sum \lambda_i a_{ji} x_j \right\| < \varepsilon/2$$

and

$$\left\| \sum \lambda_i a_{ji} x_j \right\| = \left\| \sum_{j=1}^{n} \left(\sum_{i=1}^{n+1} a_{ji} \lambda_i \right) x_j \right\| < \varepsilon/2.$$

Hence $\sum \|\lambda_i u_i\| < \varepsilon$, a contradiction. □

Theorem 5 raises a question: When is a finitely generated subspace located? A subspace of a finite-dimensional normed space is located if and only if it is finite dimensional. However, the span of a single vector in an infinite-dimensional Hilbert space can be located without being finite-dimensional: consider the vector $\sum \frac{1}{n} a_n e_n$ where e_n is an orthonormal basis, and a_n is a binary sequence that contains at most one 1.

4. Strictly convex normed spaces

Let V be a normed vector space over a subfield of the complex numbers. Following Bishop [1, Corollary page 256] we say that V is (uniformly) **strictly convex** if for each $\varepsilon > 0$, there exists $r < 1$ so that if u and v are unit vectors, and $\|u - v\| \geq \varepsilon$, then $\left\| \frac{1}{2}(u+v) \right\| \leq r$.

Hilbert spaces are strictly convex because

$$\|u+v\|^2 + \|u-v\|^2 = 2\|u\|^2 + 2\|v\|^2,$$

so if $\|u\| = \|v\| = 1$, then

$$\left\| \frac{u+v}{2} \right\| = \sqrt{1 - \frac{1}{4}\|u-v\|^2} \leq \sqrt{1 - \left(\frac{\varepsilon}{2}\right)^2} \leq 1 - \frac{\varepsilon^4}{32}$$

and we can take $r = 1 - \varepsilon^4/32$.

Any complete located subspace S of a strictly convex normed space X is strongly reflective—in fact, S is **proximinal**: each $x \in X$ has a closest point in S. This was proved for finite-dimensional subspaces in [2, 3.1 Theorem]. We shall prove the general result, without using countable choice. First we put strict convexity in a more usable form.

Lemma 6. *Let V be a strictly convex normed space. Then for each $\varepsilon > 0$ there exists $\delta > 0$ such that if $1 \leq \|u_i\| \leq 1 + \delta$ for $i = 1, 2$, and if $\left\|\frac{1}{2}(u_1 + u_2)\right\| \geq 1$, then $\|u_1 - u_2\| \leq \varepsilon$.*

Proof. Choose $r < 1$ so that if u and v are unit vectors, and $\|u - v\| \geq \varepsilon/2$, then $\left\|\frac{1}{2}(u + v)\right\| \leq r$. Choose

$$\delta < \min\left(1 - r, \frac{\varepsilon}{4}\right)$$

and let $u_i' = u_i / \|u_i\|$. To show that $\|u_1 - u_2\| \leq \varepsilon$, assume that $\|u_1 - u_2\| > \varepsilon$. Then

$$\|u_1' - u_2'\| \geq \|u_1 - u_2\| - \|u_1' - u_1\| - \|u_2' - u_2\| > \varepsilon - 2\delta > \varepsilon/2$$

so

$$r \geq \left\|\frac{u_1' + u_2'}{2}\right\| \geq \left\|\frac{u_1 + u_2}{2}\right\| - \delta \geq 1 - \delta > r,$$

a contradiction which shows that $\|u_1 - u_2\| \leq \varepsilon$. □

Theorem 7. *Let Y be a complete located subspace of a strictly convex normed space, and let x be a point at a distance d from Y. Then there exists a unique y_0 in Y such that $\|x - y_0\| = d$. So Y is strongly reflective.*

Proof. To approximate y_0 within ε, note that either $d > 0$ or $d < \varepsilon/4$. If $d < \varepsilon/4$, choose y such that $\|x - y\| < \varepsilon/2$. If $d > 0$, we may assume that $d = 1$. Choosing $\delta < \varepsilon/4$ as in the lemma, and y such that $\|x - y\| < 1 + \delta$, consider the sets

$$S_\varepsilon = \{y \in Y : d < \varepsilon/4 \text{ and } \|x - y\| < \varepsilon/2\} \cup \{y \in Y : d > 0 \text{ and } \|x - y\| < d + \delta\}.$$

These are nonempty, nested, and of diameter at most ε. Hence determine an element y_0 of Y that is within ε of each element of S_ε.

The uniqueness follows easily from strict convexity. □

Corollary 8. *In a strictly convex normed space over the real or complex numbers, linear independence is the same as metric independence.*

Proof. Note that a finite metrically independent family over the real or complex numbers spans a complete located subspace. We induct on the number of elements in the family $x_1, \ldots, x_n$, so we may assume that $x_1, \ldots, x_{n-1}$ are metrically independent and span a complete located subspace Y. Let d be the distance from x_n to Y, and

$$y_0 = \sum_{i=1}^{n-1} a_i x_i$$

be as in the theorem. Then $x_n - y_0 \neq 0$ by independence, so x_n is bounded away from Y; whence $x_1, \ldots, x_n$ are metrically independent. □

5. A weak countable choice principle

The following choice principle suffices to derive Bishop's principle and to prove the fundamental theorem of algebra. It is implied by countable choice and by the law of excluded middle.

WCC. Given a sequence A_n of nonempty sets, at most one of which is not a singleton, then there is a choice sequence $a_n \in A_n$.

What does it mean for at most one of the A_n not to be a singleton? One possibility is that if $x, y \in A_n$ and $x', y' \in A_{n'}$ with $n \neq n'$, then either $x = y$ or $x' = y'$. We will use the (possibly) stronger condition—giving a weaker axiom—that if $n \neq n'$, then either A_n or $A_{n'}$ is a singleton.

Lemma 9. *Suppose WCC. If r is a real number, then there exists a binary sequence λ_n such that $r \neq 0$ if and only if $\lambda_n = 1$ for some n. In fact, if $\lambda_n = 0$, then $|r| < 1/2n$, and if $\lambda_n = 1$, then $|r| > 1/(2n+1)$.*

Proof. Consider the sequence of nonempty sets

$$\Lambda_n = \{0 : |r| < 1/2n\} \cup \{1 : |r| > 1/(2n+1)\}.$$

It is easily seen that if $n \neq n'$, then either Λ_n or $\Lambda_{n'}$ is a singleton. So, by WCC, there exists a sequence $\lambda_n \in \Lambda_n$. □

Clearly WCC is implied by countable choice. To derive it from the law of excluded middle, note first that if all the sets A_n are singletons, there is no problem. Otherwise, let m be the index of the nonsingleton, let a_m be an element of A_m, and for $n \neq m$ let a_n be the unique element of A_n. So WCC is classically true without any choice principle.

Theorem 10. *WCC entails Bishop's principle.*

Proof. Let Y be a nonempty, complete, located subset of a metric space, and x a point. We may assume that $d(x,Y) < 1$. Using Lemma 9, construct a binary sequence λ_n such that

$$\begin{array}{lcl} \lambda_n = 0 & \Rightarrow & d(x,Y) < 1/2n, \\ \lambda_n = 1 & \Rightarrow & d(x,Y) > 1/(2n+1). \end{array}$$

Let

$$S_n = \{y \in Y : d(x,y) < 1/2n\}.$$

Note that S_n is nonempty if $\lambda_n = 0$. Now define $B_n = \{\infty\}$ unless $\lambda_n = 0$ and $\lambda_{n+1} = 1$, in which case take $B_n = S_n$. By WWC, there exists $b_n \in B_n$. Let

$$C_n = \begin{cases} S_n & \text{if } \lambda_n = 0, \\ \{b_m\} & \text{if } \lambda_n = 1, \text{ where } \lambda_m = 0 \text{ and } \lambda_{m+1} = 1. \end{cases}$$

The diameter of C_n is at most $1/n$, so the sequence (C_n) defines a point y_0 in Y that is within $1/n$ of any point in C_n. If $x \neq y_0$, then there exists n such that $d(x, y_0) > 2/n$, so $d(x, C_n) > 1/n$. Thus $\lambda_n = 1$, and therefore $d(x,Y) > 1/(2n+1)$. □

We conclude by outlining how WCC suffices to construct individual roots for the fundamental theorem of algebra. First consider the problem of constructing a root of $X^2 - a$. Using Lemma 9, construct a binary sequence λ_n such that

$$\begin{array}{lcl} \lambda_n = 0 & \Rightarrow & |a| < 1/2n, \\ \lambda_n = 1 & \Rightarrow & |a| > 1/(2n+1). \end{array}$$

Let $A_n = \{0\}$ unless $\lambda_{n-1} = 0$ and $\lambda_n = 1$, in which case let $A_n = \{x : x^2 = a\}$, a two-element set. Another application of WCC gives, for each n, a point $a_n \in A_n$. Finally, if $\lambda_m = 1$, redefine a_m to be a_n, where $\lambda_{n-1} = 0$ and $\lambda_n = 1$. This gives a Cauchy sequence converging to a root of $X^2 - a$.

Now consider the fundamental theorem of algebra for any monic polynomial of degree $n > 0$. A **multiset** of size n of complex numbers is a finite sequence $z_1, \ldots, z_n$. The **distance** between two multisets $z_1, \ldots, z_n$ and $w_1, \ldots, w_n$ is the infimum, over all permutations σ of $\{1, \ldots, n\}$, of $\sup_i |z_i - w_{\sigma i}|$. This gives a metric space $M_n(\mathbf{C})$. The elements of the completion $\widehat{M_n}(\mathbf{C})$ need not be multisets, but they are approximated by multisets. To each element μ of $\widehat{M_n}(\mathbf{C})$ there corresponds a unique monic polynomial f of degree n, and the multisets approximating μ give complete factorizations of approximations to f. The choiceless constructive fundamental theorem of algebra says that, conversely, given a monic polynomial f of degree n, there exists $\mu \in \widehat{M_n}(\mathbf{C})$ (the spectrum of f) to which f corresponds, see [5].

To prove the fundamental theorem of algebra in its traditional form, we must construct a point in μ. Let d be the diameter of μ. Using Lemma 9, construct a binary sequence λ_n such that

$$\begin{aligned} \lambda_n = 0 \quad &\Rightarrow \quad d < 1/2n, \\ \lambda_n = 1 \quad &\Rightarrow \quad d > 1/(2n+1). \end{aligned}$$

Let $A_n = \{\infty\}$ unless $\lambda_{n-1} = 0$ and $\lambda_n = 1$, in which case let A_n be the set of all nontrivial ordered partitions of μ into two separated elements μ_1 and μ_2. Such a partition gives a factorization of the polynomial f. By induction on degree, the set of roots of these factors is nonempty, so we can proceed as in the quadratic case.

References

[1] Bishop, Errett, *Foundations of constructive analysis*, McGraw-Hill, 1967.

[2] Bridges, Douglas S., On the foundations of best approximation theory, *J. Approx. Thry.* **28**(1980), 273–292.

[3] Heyting, Arend, *Intuitionism, an introduction*, North-Holland, 1971

[4] Mines, Ray, Fred Richman and Wim Ruitenburg, *A course in constructive algebra*, Springer-Verlag, 1988.

[5] Richman, Fred, The fundamental theorem of algebra: a constructive development without choice, `http://www.math.fau.edu/Richman/html/docs.htm`

[6] Scedrov, Andre, Diagonalization of continuous matrices as a representation of intuitionistic reals, *Annals of Pure and Applied Logic*, **30**(1986), 201–206.

Department of Mathematics
Florida Atlantic University
Boca Raton, FL 33431
`richman@acc.fau.edu`