Applications of a Quasireflexive R Sequence of Banach Spaces

ANDREW B. PERRY
Dept. of Mathematics and Computer Science
Springfield College
263 Alden St., Springfield MA 01109
United States of America

Abstract: We make use of the James space to exhibit an R sequence of Banach spaces which contains infinitely many quasireflexive spaces. There are natural applications of this construction to cryptography and error correcting codes.

Key-Words: Banach Space, R Sequence, James Space, Encryption, Cyrptography,Security, Error Correcting Code, Erasure Channel

1 Introduction

R sequences are useful in studying the interrelationships between Banach Spaces and their subspaces, but few direct applications of these sequences have been discovered [8]. In 1951 R.C. James discovered a nonreflexive separable Banach Space such that there is an isomorphism between J and J** [6]. In this paper we make use of the James space to construct an R sequence containing infinitely many quasi- reflexive spaces. We can exploit this property to develop a system of cryptography which, though difficult to implement, could be extremely secure.

2 R Sequences

A Banach space X is said to be quasireflexive (of order k) if the quotient of X** by the natural image of X in X** has finite dimension (dimension k).

Let $\{X_i\}$ be a sequence of Banach Spaces. For integers j, k, with j < k, let $A_{j,k}$ be a Banach Space (called a transition space). Let $f_{j,k} : X_j \to A_{j,k}$ and $g_{j,k}$: $A_{j,k}$ k -> X_k be bounded linear functions (called transition functions).Let C_k be the cardinality of the set $\{a: a < k , X_a$ is reflexive $\}$.

We say that X_i is a CR sequence of Banach Spaces if the following conditions hold:

First, we require that $\lim (k \to \infty) C_k / k = 1$.

Second, if $j_1 < j_2$ and $k_1 < k_2$, then

$0 \leq \| f\_(j_1,k_1) \| \leq 1$ and

$0 \leq \| g\_(j_2,k_2) \| \leq 1$.

We say that a CR sequence is an R sequence if in addition, for every if $j_1 < j_2$ and $k_1 < k_2$, then

$0 < \| f\_(j_1,k_1) \|$ and

$0 < \| g\_(j_2,k_2) \|$.

The primary goal of this paper is to construct an R sequence in which infinitely many of the spaces X_i are quasireflexive.

3 James Space

We first present some background on the James space. For its definition, the reader may consult [6] or almost any modern book on Banach Space Theory, such as [4] or [12].

It is easy to verify that J is a Banach space. James also proved that this space enjoys the following properties. J is separable, its unit vector basis of J is shrinking and it is is quasireflexive of order 1 .J is isometrically isomorphic to its second dual J**.The successive duals J*, J**, ... are separable, and therefore J cannot have subspaces isomorphic to c_0 or l_1. J is not isomorphic to a subspace of a space with unconditional basis.

Let A be a nonempty, separable, weakly closed subset of the unit ball of a Banach space X. Then the following are equivalent [11].

(1) The set A is not weakly compact

(2) there is a θ for which $0 < \theta < 1$ and a sequence $(x_n)^* \in B_{X^*}$ such that $\lim (k \to \infty)\ (x_n)^*x = 0$ for each x in A and $\sup \{ |x^*x| : x \in A\} \geq \theta$ whenever x^* Ų $co(\{ x_n^*: n \in \mathbf{N}\})$.

(3) There is a $z^* \in X^*$ such that $\sup \{ |z^*x| : x \in A \}$ is not attained.

We outline here James' proof [7] that (1) implies (2) because of its potential implications for the application of a quasireflexive R sequence to strong cryptography. Suppose that A is not weakly compact. Let V = |A| and let W be the vector space underlying V* but with the norm given by the formula $||v^*||_W$ = sup{ |v*x| : x in A }. Since a member of W that is a zero on A must be a zero on V, we can see that ||.|| is really a norm on W. Let f: A -> W be defined by the formula (f(x))(v*) = v*x; that is, let f be the "natural map" from A in to W*.

Now since V* is a separating family of linear functionals on V, the function is one-to-one. James applies Helly's theorem [5] to concluded the desired result.

4 An R sequence containing infinitely many quasireflexive spaces

Denote by J_n the l_2 direct sum of n isomorphic copies of the James space, that is,
$J_n = (J + J + ... + J)_2$.

Bessaga and Pelcynski [2] proved that if X and Y are quasireflexive Banach Spaces of order m and n , repectively, then X + Y is quasireflexive of order m+n .

It follows that the spaces J_n are pairwise non-isomorphic.

We first partition the positive integers as follows:
let P be the set of all integers of the form
P = ∑ (i=1,n) i for some integer n,
and let Q be the complement of this set in the integers.
If n is in P, and if n = ∑ (i=1,m) i , then let X_n = J_m..
If n is in Q, we let $X_n = l_p$ where p=2- 1/n.

If j,k is in P then let A_(j,k) = J, and let f_(j,k) and g_(j,k) be the identity maps on J.

If j is in P and k is in Q, then let
A_(j,k) = **R**. Let f_(j,k)(x)= | x |
, and let g_(j,k) = (x,x,x, ...) .

If j, k is in Q then let A_(j,k) = l_q where q= 2 - 1/j.
Let f_(j,k): l_q -> l_q
and g_(j,k): l_q -> l_(2- 1/k)
each be the identity maps.

If j is in P and k is in Q, then
let A_(j,k) = l_2. We can let f_(j,k): J -> l_2
and g_(j,k): l_2 -> l_(2- 1/k) be identity maps. (It is easy to see that these maps are bounded.)

Noting that all l_p spaces with $1 \leq p \leq 2$ are reflexive, it is easy to verify that the sequence X_i of Banach Spaces defined above, with transition sets and transition functions defined above, is an R-sequence with infinitely many quasireflexive spaces.

5 Applications to Cryptography and Error Correcting Codes

We outline steps by which this theory could theoretically be put into practice.

First an R sequence must be chosen with sufficiently many quasireflexive spaces that security to make the cost of decryption prohibitively high. In the construction found here only finitely many spaces are non-quasireflexive. Second, an invertible map P_i must be chosen between plaintext characters (bits or bytes) and elements of each space X_i. Of course, this is possible due to the axiom of choice. Call the inverse functions Q_i. Finally, sender and receiver must agree on which transition maps to employ.

A plaintext message could be interpreted as a sequence of elements of the Banach Spaces $(x_1,x_2,x_3,...)$. For added security a key $(y_1,y_2,y_3,...)$ could be chosen in advance. Sender would apply the functions P_i to his initial message, and then send the bitstream $(Q_1(x_1+y_1),Q_2(x_2+y_2),...)$ via an insecure channel.

Luby, Mitzenmacher, Shokrollahi, and Spielman [9] recently discovered a simple erasure recovery algorithm for codes derived from cascades of sparse bipartite graphs. They adopted as their model of errors the erasure channel introduced by Elias [3], in which each codeword symbol is lost with a fixed constant probability *p* in transit independent of all the other symbols. Elias showed that the capacity of the erasure channel is *1-p* and that a random linear code can be used to transmit over the erasure channel at any rate *R < 1-p.* An R sequence with infinitely many quasireflexive spaces could applications in this research area as well.

References:

[1] N. Alon and M. Luby, A linear time erasure-resilient code with nearly optimal recovery, *IEEE Trans. Inform. Theory*, Vol. 42, 1996, pp. 1732-1736.

[2] C. Bessaga and A. Pelczynski, A generalization of results of R.C. James concerning absolute bases in Banach Spaces, *Studia Math.* 17, 1958, pp. 151-164.

[3] P. Elias, "Coding for two noisy channels", in *Information Theory, 3rd London Symp.,* 1955, pp.61-76.

[4] P. Habala, P. Hajek, and V. Zizler, *Introduction to Banach Spaces*, Matfyz Press, 1996.

[5] E. Helly, Über Systeme linearer Gleichungen mit unendlich vielen Unbekannten, *Montash. Math. Phys*., Vol. 31, 1921, pp. 60-91.

[6] R.C. James, A non-reflexive Banach space isometric with its second conjugate space, Proc. nat. Acad. Sci. USA, Vol. 37, 1951, pp. 159-169.

[7] R.C. James, Reflexivity and the sup of linear functionals, *Israel J. Math*., Vol .13, 1972, pp. 289-300.

[8] J. Lindenstrauss and L. Tzafriri, *Classical Banach Spaces I and II,* Springer-Verlag, 1977.

[9] M. Luby, M. Mizenmacher, M. Shokrollahi, and D. Spielman, Efficient Erasure Correcting Codes, *IEEE Trans. Inform. Theory*, Vol. 47, No.2 , 2001, pp. 569-583.

[10] D. Mackay, S. Wilson, and M. Davey, Comparison of constructions of irregular Gallager codes, *IEEE Trans. Commun*., Vol. 47, No. 10, 1999, pp. 1449-1454.

[11] B. Maurey and H. Rosenthal, Normalized weakly null sequences with no unconditional subsequences, *Studia Math.* 61 (1977),pp. 77-98.

[12] R. Megginson, *An Introduction to Banach Space theory,*Springer-Verlag, 1998.

[13] H. Royden, *Real Analysis*, Prentice Hall, 1988.