UPPER BOUNDS FOR THE SPAN OF PROJECTIVE STIEFEL MANIFOLDS

Parameswaran Sankaran
Institute of Mathematical Sciences,
CIT Campus, Taramani, Chennai 600 113
India
and
Peter Zvengrowski
Department of Mathematics & Statistics
University of Calgary
Calgary, Alberta, T2N 1N4
Canada
Email: sankaran@imsc.res.in
zvengrow@ucalgary.ca

Research of both authors was partially supported by NSERC of Canada
2000 A.M.S. Subject Classification:- 57R25, 55S25
Key words and phrases: Projective Stiefel manifolds, vector fields, K-theory

Dedicated to Professor Samuel Gitler
on the occasion of his seventieth birthday

Abstract: We obtain upper bounds for the span of projective Stiefel manifolds $X_{m,k}$ when $2 \leq k \leq \lfloor m/2 \rfloor$ using the description of the (stable) tangent bundle and the complex K-ring of these manifolds, as well as the universal property these manifolds enjoy, i.e. $X_{m,k}$ is a classifying space for line bundles whose m-fold Whitney sum with itself admits k everywhere linearly independent sections. We also exhibit examples in which these upper bounds are compared with the respective known lower bounds.

1 Introduction

The Stiefel and projective Stiefel manifolds, written respectively $V_{m,k}$, $X_{m,k}$, and defined in the next paragraph, have been a recurring theme in the work of S. Gitler (unless otherwise stated we are always referring to the real Stiefel and real projective Stiefel manifolds). In a 1970 monograph with K.Y. Lam the first computations of the complex K-theory of the Stiefel manifolds was carried out, cf. [11] and also A. Roux [19]. A little earlier, in 1968, Gitler and D. Handel defined and studied the projective Stiefel manifolds, cf. [9], [10]. In the 1970's this work was carried further by Gitler's student E. Antoniano, cf. [2], leading to the 1986 paper [3] by Antoniano, Gitler, J. Ucci, and P. Zvengrowski in which the complex K-theory of these spaces was computed, for $m = 4n$, and as an application the parallelizability of all $X_{m,k}$ was settled apart from the single exception $X_{12,8}$. This work was generalized in 1996-2000 by N. Barufatti and D. Hacon (cf. [6], [7]), where $K^*(X_{m,k})$ was computed for all m. The K-theory of the projective Stiefel manifolds has a much richer structure than that of the Stiefel manifolds, and the purpose of this note is to take advantage of this richer structure, in particular the ring structure, to obtain strong upper bounds for the span (also defined in the next paragraph) of $X_{m,k}$, at least in a relatively large number of cases. We also give examples where this upper bound is within 1 of the known lower bound, thus giving a nearly exact determination of the span. The interest of Gitler in projective Stiefel manifolds has been ongoing, we simply mention two recent papers on the complex projective Stiefel manifolds [4], [5].

Let m, k be positive integers with $k < m$. Recall that the Stiefel manifold $V_{m,k}$ is the space of all orthonormal k-frames in $\mathbb{R}^m$ and can be realized as the homogeneous space $SO(m)/SO(m-k)$, which gives it a natural structure as a smooth manifold of dimension $d_{m,k} := \binom{m}{2} - \binom{m-k}{2} = mk - \binom{k+1}{2}$. The projective Stiefel manifold $X_{m,k}$ is the smooth manifold of the same dimension, obtained as the quotient of $V_{m,k}$ by the action of $\mathbb{Z}/2$ given by the antipodal involution $(v_1, \cdots, v_k) \mapsto (-v_1, \cdots, -v_k)$. The topology of projective Stiefel manifolds has been studied extensively. We refer the reader to [22] for a more detailed discussion and relevant references.

Recall that for a vector bundle γ over a base space X, span of γ is the largest integer r such that γ admits r everywhere linearly independent sections. When X is a smooth manifold span(X) is defined to be the span of its tangent bundle τ_X, and the stable span, span$^0(X)$, is defined to be span$(\tau_X \oplus q\varepsilon) - q$ for some (indeed any) $q \geq 1$, where $q\varepsilon$ denotes the trivial bundle of rank q. If X has dimension n then clearly

$$0 \leq \operatorname{span}(X) \leq \operatorname{span}^0(X) \leq n .$$

Our main theorem yields upper bounds for span$^0(X_{m,k})$ (and thereby also for span$(X_{m,k})$), for $k < \lfloor m/2 \rfloor$. Our main tool is the complex K-theory $K^*(X_{m,k})$, in particular its ring structure, and the following well-known (cf. [9], [21]) universal property of $X_{m,k}$. If ξ is any line bundle over a base space X such that span of $n\xi$ is $r \geq 1$, then ξ is isomorphic to $f^*(\xi_{n,r})$, for some continuous map $f : X \longrightarrow X_{n,r}$, where $\xi_{n,r}$ is the Hopf line bundle which is associated to the double covering $V_{n,r} \longrightarrow X_{n,r}$. (Usually it is assumed that X has the homotopy type of a finite CW-complex or that ξ admits a Euclidean metric, however the universal property holds without any further hypothesis on X, cf. [8].)

We postpone to a later paper a detailed treatment of lower bounds for the (stable) span of $X_{n,r}$ and other approaches to obtaining upper bounds as the methods involved are varied and quite different in spirit from the present one. However, for the present, we refer the reader to [13], [14], [22], and also to the brief treatment given in §4 of the present note. We also mention that precise results for span$(X_{m,k})$ have been obtained for "large" k close to m (explicitly, for $k = m-1, m-2, m-3$) by Zvengrowski [23]. In contrast, the results of the present paper hold for $k < \lfloor m/2 \rfloor$.

We now state the main theorem of this paper. Note that $X_{n,1} \cong P^{n-1}$, the real projective space of dimension $n-1$. We omit this case, the solution for which is well-known and classical [1].

Theorem 1.1. *Let $k > 2$ and $m = 2n$ (in (i)) or $m = 2n + 1$ (in (ii) and (iii)). As above, write $d_{m,k} = \dim(X_{m,k})$.*
(i) One has $span^0(X_{2n,k}) \leq d_{m,k} - (2q + 2)$, if $k \leq n - 1$ and $(-1)^q\binom{nk-1}{q}$ is not a quadratic residue mod 2^{n-2q}.
(ii) When $k = 2s$, $span^0(X_{2n+1,2s}) \leq d_{m,k} - 2q - 2$ if $k < n$ and $(-1)^{s-q}\binom{ms-1}{q}$ is not a quadratic residue mod 2^{n-2q}.
(iii) When $k = 2s + 1$, $span^0(X_{2n+1,2s+1}) \leq d_{m,k} - 2q$ if $k < n, q < s - 1, n \geq 3q$ and $(-1)^{N-q}\binom{N}{q}$ is not a quadratic residue mod 2^{n-3q}, where $N = (mk - 1)/2$.

For $n \equiv 0 \pmod 4$, the result of our main theorem was stated in [13] without proof. We recall the description due to Barufatti-Hacon [7] of the complex K-ring of projective Stiefel manifolds in §2. We take up the proof of the main theorem in §3. In §4, as mentioned above, we give a brief discussion of lower bounds, some examples to illustrate our theorem, and make some concluding remarks. A short number theoretical appendix about quadratic residues modulo 2^n is added, since these will occur in any application of the main theorem.

Acknowledgements: The authors wish to thank Renate Scheidler for useful discussions regarding the appendix of this paper. In particular Proposition 5.4 is due to her.

2 The K-ring of projective Stiefel manifolds

The structure of the complex K-ring $K^*(X_{m,k})$, as mentioned in the Introduction, was first determined in [3] for $m = 4n$, using the Hodgkin spectral sequence. This work was extended to all m by N.Barufatti and D.Hacon [7], giving a complete determination of the ring $K^*(X_{m,k})$, with the exception that when mk is odd, only $K^0(X_{m,k})$ has been determined. We now recall their results on the ring structure of $K^0(X_{m,k})$ as this is what is needed for our purposes (we shall not need K^1, and of course $K^2 \approx K^0$ by Bott periodicity). For the structure of $K^*(V_{m,k})$ we refer the reader to [11]. In what follows, we often identify a vector bundle γ with its class $[\gamma]$ in the K-ring, and also write K for K^0.

Recall that $\xi_{m,k}$ denotes the real line bundle associated to the double covering $V_{m,k} \longrightarrow X_{m,k}$. Let $y = [\xi_{m,k} \otimes \mathbb{C}] - 1 \in K(X_{m,k})$. Note that $X_{m,k}$

can be expressed as the homogeneous space $Spin(m)/H$, where the connected component of H containing 1 is $Spin(m-k)$ which has index 2 in H. Denote by D (resp. D^+) the (complex) spin representation of $Spin(m-k)$ when $m-k$ is odd (resp. 'the' half-spin representation when $m-k$ is even). One can show that D actually affords a representation of H itself which restricts to the spin representation of $Spin(m-k)$. A similar statement holds for D^+ when $m-k$ is even. The α-construction applied to D then yields vector bundles over $X_{m,k}$ denoted $\mathbb{D}$ (resp. $\mathbb{D}^+$ when m is even). Denote by δ (resp. δ^+) the element $[\mathbb{D}] - rank(\mathbb{D}) = [\mathbb{D}] - 2^c$ (resp. $[\mathbb{D}^+] - 2^{c-1}$) where $c = \lfloor m-k/2 \rfloor$.

Notations: For any positive integer k, let $\nu_2(k)$ denote the highest exponent of 2 which divides k. Define $\alpha_{2n,k} = \min\{n-1, 2i-1+\nu_2\binom{n}{i} \mid i > \lfloor 2n-k/2 \rfloor\}$, $\alpha_{2n+1,2s} = \min\{n, 2i-1+\nu_2\binom{n}{i} \mid i > n-s\}$, and, $\alpha_{2n+1,2s+1} = \min\{\alpha_{2n+1,2s}, 2(n-s)+\nu_2\binom{n}{s}\}$. We shall write α for $\alpha_{m,k}$ when there is no risk of confusion.

Theorem 2.1. *(Barufatti-Hacon [7]) With the above notations, we have*

(EO): The ring $K(X_{2n,2s-1}) = \mathbb{Z}[y,\delta]/\sim$ where the ideal of relations is generated by
(i) $y^2+2y, 2^\alpha y, 2^{s-1}\delta$, and, $\delta^2 + 2^{n-s+1}\delta - 2^{2n-2s-1}(1-(-1)^s\binom{n-1}{n-s})y$.

(EE): The ring $K(X_{2n,2s}) = \mathbb{Z}[y,\delta,\delta^+]/\sim$ where the ideal of relations is generated by elements (i) above and
(ii) $(\delta^+)^2 - \delta\delta^+ + 2^{2n-2s-3}(1+(-1)^s\binom{n-1}{s})y - 2^{n-s-1}\delta$.

(OE): The ring $K(X_{2n+1,2s}) = \mathbb{Z}[y,\delta]/\sim$ where the ideal of relations is generated by
(iii) $y^2+2y, 2^\alpha y, 2^{s-1}(y+2)\delta + 2^{n-1}y$, $\delta^2 + 2^{n-s+1}\delta - 2^{2n-2s-1}(1-(-1)^s\binom{n}{s})y$.

(OO): The ring $K(X_{2n+1,2s+1}) = \mathbb{Z}[y,\delta]/\sim$ where the ideal of relations is generated by
(iv) $y^2+2y, 2^\alpha y, y\delta + 2^{n-s}y, 2^s\delta$ and $\delta^2 + 2^{n-s+1}\delta - 2^{2n-2s-1}(1-\binom{n}{s})y$. □

Remark 2.2. (i) Note that $2^{n-1}y = 0$ in $K(X_{2n,k})$. In fact 2^{n-1} is the (additive) order of y when $k < n$, since in that case, $\alpha_{2n,k} = n-1$. Likewise, $2^n y = 0$ in $K(X_{2n+1,k})$ and the order of $y \in K(X_{2n+1,k})$ is 2^n, since $\alpha_{2n+1,k} = n$ when $k \leq n$ (see also properties of the "lower range" in [8]).
(ii) The ring $K(X_{2n,2s})$ is naturally an algebra over $K(X_{2n,2s-1})$ via the map induced by the projection $X_{2n,2s} \longrightarrow X_{2n,2s-1}$. It is readily seen from the above theorem that $K(X_{2n,2s})$ is a free $K(X_{2n,2s-1})$ module with basis $1, \delta^+$. However, $K(X_{2n+1,2s+1})$ is not in general a free module over $K(X_{2n+1,2s})$.

Nevertheless, under the map induced by the projection, the elements $y, \delta \in K(X_{2n+1,2s})$ map to $y, \delta \in K(X_{2n+1,2s+1})$ respectively.

3 Proof of Main Theorem

The proof of the main theorem will be based on the following proposition. It will be convenient to denote the generators of $K(X_{2N,2S-1})$ given by Theorem 2.1 as Y, Δ. Similar notations will be used in the case of $K(X_{2N+1,2S})$ etc. We also recall the standard surjective homomorphism, for any space X, $rank : K(X) \twoheadrightarrow \mathbb{Z}$, where for any rank n vector bundle β over X, $rank[\beta] = n$.

We shall make extensive use of the relations in the K-ring of projective Stiefel manifolds given in Theorem 2.1 throughout the proof of the following proposition without specific mention.

Proposition 3.1. *Let $2 \leq k < n < S < N$, and let $q := N - S < n$.*

(i) Suppose that $(-1)^q\binom{N-1}{q}$ is not a quadratic residue mod 2^{n-2q}. Then, for any ring homomorphism $\varphi : K(X_{2N,2S-1}) \longrightarrow K(X_{2n,k}), k = 2s-1, 2s$, which preserves rank, $\varphi(Y) \neq y$.

(ii) Let $k = 2s$. Suppose that $(-1)^S\binom{N-1}{q}$ is not a quadratic residue mod 2^{n-2q}. Then for any ring homomorphism $\varphi : K(X_{2N,2S-1}) \longrightarrow K(X_{2n+1,2s})$ which preserves rank, one has $\varphi(Y) \neq y$.

(iii) Let $k = 2s+1$. Suppose that $q \leq s-1$ and $n \geq 3q+1$. If $(-1)^S\binom{N}{q}$ is not a quadratic residue mod 2^{n-3q+1}, then for any rank preserving ring homomorphism $\varphi : K(X_{2N+1,2S+1}) \longrightarrow K(X_{2n+1,2s+1})$, one has $\varphi(Y) \neq y$.

Proof: (i) Assume that $k = 2s-1$. Since $k < n$ we have $s-1 \leq n-s-1$ and $2n-2s-1 \geq n-1$. Hence $\delta^2 = 0$ in $K(X_{2n,k})$. Suppose that $\varphi(Y) = y$. Write $\varphi(\Delta) = a\delta + b\delta y + cy$. Then $\varphi(\Delta^2) = (a\delta + b\delta y + cy)^2$. Since $y^2 = -2y$ and $\delta^2 = 0$, we get $\varphi(\Delta^2) = -2c^2y + 2ac\delta y - 4bc\delta y$. Applying φ to both sides of the relation $\Delta^2 = -2^{N-S-1}\Delta + 2^{2N-2S-1}(1 - (-1)^S\binom{N-1}{q})Y$, we obtain

$$-2c^2y + 2c(a-2b)\delta y = -2^{q-1}(a\delta + b\delta y + cy) + 2^{2q-1}y - 2^{2q-1}(-1)^S\binom{N-1}{q}y.$$

Equating the terms containing y leads to $2^{2q-1}(-1)^S\binom{N-1}{q}y = 2(c - 2^{q-1})^2y$. Since the order of y is 2^{n-1} this implies that $2^{2q-1}(-1)^S\binom{N-1}{q} \equiv 2(c - 2^{q-1})^2$

mod 2^{n-1}. Hence $(c-2^{q-1})^2 = 2^{2q-2}u^2$ for some integer u. On dividing throughout by 2^{2q-1} we get $(-1)^S\binom{N-1}{q} \equiv u^2 \bmod 2^{n-2q}$ and so $(-1)^S\binom{N-1}{S}$ is a quadratic residue mod 2^{n-2q}.

Now let $k = 2s$. Since $k < n$, we have as before $\delta^2 = 0$ in $K(X_{2n,2s})$. We claim that $(\delta^+)^2 = \delta\delta^+$. To see this note that $2n-2s-3 = 2n-k-3 = n-2+(n-1-k) \geq n-2$ with equality only if $n = 2s+1$ in which case $\binom{n-1}{s}$ is even. Since the order of y is 2^{n-1}, it follows that $(\delta^+)^2 = \delta\delta^+$. Therefore we have a $K(X_{2n,2s-1})$-algebra homomorphism $\theta : K(X_{2n,2s}) \longrightarrow K(X_{2n,2s-1})$ defined by $\delta^+ \mapsto 0$ which restricts to the identity on $K(X_{2n,2s-1}) \subset K(X_{2n,2s})$. The composition $\theta \circ \varphi : K(X_{2N,2S-1}) \longrightarrow K(X_{2n,2s-1})$ is then a rank preserving ring homomorphism which maps Y to $\varphi(y)$. By what has been shown already, $\varphi(Y) \neq y$ if $(-1)^q\binom{N-1}{q}$ is not a quadratic residue mod 2^{n-2q}.

(ii): Note that since $2s = k < n$, we see that the order of y is 2^n. Also $2n-2s-1 \geq n$, so $\delta^2 = -2^{n-s-1}\delta$. Suppose that $\varphi(Y) = y$. Write $\varphi(\Delta) = a\delta + b\delta y + cy$. Applying φ to both sides of the relation $\Delta^2 = -2^{q+1}\Delta + 2^{2q-1}(1-(-1)^S\binom{N-1}{S})Y$ we obtain

$$-2c^2y + \lambda\delta = -2^{q+1}(a\delta + b\delta y + cy) + 2^{2q-1}(1-(-1)^S\binom{N-1}{q})y,$$

where $\lambda = 2c(a-2b)y - 2^{n-s+1}a^2 - 2^{n-s-2}aby$.

Let $R = \mathbb{Z}[y]/\langle y^2+2y, 2^{n-1}y\rangle$. Now using 2.1(OE), we see that the there is a well defined rank preserving ring homomorphism $\theta : K(X_{2n+1,2s}) \longrightarrow R$ such that $\theta(\delta) = 0, \theta(y) = y$. Applying θ to the above equation we get

$$-2c^2y = -2^{q+1}cy + 2^{2q-1}(1-(-1)^S\binom{N-1}{q})y$$

in R. This can be rewritten as $2(c-2^{q-1})^2 \equiv 2^{2q-1}(-1)^S\binom{N-1}{q} \pmod{2^{n-1}}$. This implies that $(-1)^S\binom{N-1}{q}$ is a quadratic residue mod 2^{n-2q}.

(iii): Since $2s+1 = k < n$, the order of $y \in K(X_{2n+1,2s+1})$ is 2^n. Since $n-s+1 > s$, and $2n-2s-1 \geq n$, it follows that $\delta^2 = 0$. Suppose $\varphi(Y) = y$, and in this case we can write $\varphi(\Delta) = a\delta + cy$. Applying φ to both sides of the relation $\Delta^2 = -2^{q+1}\Delta + 2^{2q-1}(1-\binom{N}{S})Y$, we get

$$2ac\delta y - 2c^2y = -2^{q+1}a\delta - 2^{q+1}cy + 2^{2q-1}(1-(-1)^S\binom{N}{S})y.$$

Since $\delta y = -2^{n-s}y$ this equation can be rewritten as

$$2^{2q-1}(-1)^S\binom{N}{S}y = 2(c-2^{q-1})^2y - 2^{q+1}a\delta + 2^{n-s+1}acy.$$

Comparing the coefficients of δ on both sides we see that 2^{s-q-1} divides a since $2^s\delta = 0$. Write $a = 2^{s-q-1}a'$. This leads to the equation $2^{2q-2}(-1)^S\binom{N}{S} \equiv (c-2^{q-1})^2 + 2^{n-q-1}a'c \pmod{2^n}$. Therefore $2^{2q-2}(-1)^S\binom{N}{S} \equiv (c-2^{q-1})^2 \pmod{2^{n-q-1}}$. It follows that $(-1)^S\binom{N}{S}$ is a quadratic residue mod 2^{n-3q+1}. $\square$

Proof of Theorem 1.1: It is well known [16] that the tangent bundle τ of $X_{m,k}$ is stably equivalent to $mk\xi_{m,k}$. Specifically

$$\tau \oplus (mk - d_{m,k})\varepsilon \approx mk\xi_{m,k}.$$

Suppose that the stable span of $X_{m,k}$ is at least $d-p$, (where $p = 2q+1$ or $2q$ according as mk is even or odd respectively). Then $mk\xi_{m,k} \approx (mk-p)\varepsilon \oplus \eta$ for a suitable vector bundle η. The universal property of $X_{mk,mk-p}$ now implies that there must be a continuous map $f : X_{m,k} \longrightarrow X_{mk,mk-p}$ such that $f^*(\xi_{mk,mk-p}) \approx \xi_{m,k}$. The rank preserving ring homomorphism $f^* : K(X_{mk,mk-r}) \longrightarrow K(X_{m,k})$ must then map $[\xi_{mk,mk-p} \otimes \mathbb{C}] - 1$ to $[\xi_{m,k} \otimes \mathbb{C}] - 1$, i.e. $f^*(Y) = y$. To complete that proof we need only show that under the hypotheses of the theorem, in each case there can be no such ring homomorphism. This follows immediately from Proposition 3.1 on taking $N = \lfloor mk/2 \rfloor$ and $S = \lfloor (mk-p)/2 \rfloor$. Note that $q = N - S$ in each case. $\square$

Remark 3.2. (i) Since the tangent bundle of $X_{m,k}$ is stably isomorphic to $mk\xi$, it follows that the normal bundle with respect to any immersion of $X_{m,k}$ in Euclidean space is stably equivalent to $2^\alpha - mk\xi$. The above proposition can again be used to obtain non-immersion results by taking $N = 2^a - mk$ where $a \geq \alpha(m,k)$ is sufficiently large so that $N > n$.
(ii) The above proposition also implies non-existence of equivariant maps between the corresponding Stiefel manifolds. Indeed if $\widetilde{f} : V_{m,k} \longrightarrow V_{M,K}$ is equivariant with respect to the antipodal action of $\mathbb{Z}/2$, then one has the induced map $f : X_{m,k} \longrightarrow X_{M,K}$ which has the property that $f^*(Y) = y$, where f^* is the induced map in K theory.

4 Lower Bounds and Examples

A great deal of work has been done on determining the span of multiples of the Hopf line bundle ξ_n over P^n (also called "the generalized vector field problem"), we mention only [2], [17], [18], from the fairly extensive literature on this subject. Although the solution is by no means complete, the answer is known in most cases and hence the number $k_{n,r}$ that will now be defined is, at least in most cases, effectively computable using [17].

Definition 4.1. $k_{n,r} = -\binom{n}{r+1} + \mathrm{span}(nr\xi_{n-1})$.

Recalling that the tangent bundle τ of $X_{n,r}$ is stably $nr\xi_{n,r}$, and using the fact that under the fibre map $p : X_{n,r} \to P^{n-1}$ one has $p^*(\xi_{n-1}) = \xi_{n,r}$, it is easily seen that $k_{n,r}$ is a lower bound for $\mathrm{span}^0(X_{n,r})$. However, it is proved in [15] that in fact $\mathrm{span}(X_{n,r}) \geq k_{n,r}$, for all $n > r \geq 1$ except possibly for $r = 2$ and n odd. This gives strong lower bounds for the span, especially in the "lower range" (using the language of [8]; it is shown there that any $r < \lfloor n/2 \rfloor$ is in the lower range so the precise definition is unimportant here, the hypotheses of our main theorem imply that we are in the lower range). We now give examples that illustrate both the upper bound coming from the main theorem and the lower bound coming from $k_{n,r}$.

Example 4.2. One has (i) $12 \leq \mathrm{span}(X_{10,2}) \leq 13$,
(ii) $35 \leq \mathrm{span}^0(X_{13,4}) \leq 38$,
(iii) $25 \leq \mathrm{span}(X_{12,3}) \leq 26$,
(iv) $37 \leq \mathrm{span}(X_{12,5}) \leq 39$,
(v) $d_{16,r} - 7 \leq \mathrm{span}(X_{16,r}) \leq d_{16,r} - 6$,
where in (v) $r = 3, 5, 7$ and (as usual) $d_{16,r} = \dim(X_{16,r})$.

Proof: We illustrate (iii). Here the results of Lam [17], together with the observations preceding these examples, give the lower bound $k_{12,3} = 25$ for the span. As far as the upper bound, we simply apply Theorem 1.1 (i) with $q = 1$ and observe that $-\binom{17}{1} \equiv 15 (\mathrm{mod}\, 16)$, which is not a quadratic residue mod 16. The other proofs are similar, with $q = 1$ in (i), (ii) and $q = 2$ in (iv), (v). Finally, in (ii), the result is valid only for the stable span, again due to the observations preceding these examples. □

We remark that in general the upper bounds coming from Theorem 1.1 will not be as close to the $k_{n,r}$ lower bounds as in Examples 4.2, and for n

odd other upper bounds derived from the $\mathbb{Z}/2$ cohomology usually seem to be sharper. Nevertheless Theorem 1.1 is clearly a useful source of upper bounds, and since for $n \geq 5$ over 3/4 the numbers in $\mathbb{Z}/2^n$ are *not* quadratic residues (cf. Proposition 5.5), it follows that each application of the non-quadratic residue criterion in Theorem 1.1 has a fairly high probability of success. The following example is one illustration of this idea.

Example 4.3. Let $n = 2^t + 4,\ r = 2^l - 1,\ 2 \leq l \leq t-5$. Then

$$d_{n,r} - 2^t \leq \operatorname{span}(X_{n,r}) \leq d_{n,r} - 2^t + (2^{t-2} - 2^{l+3} + 8).$$

Proof: Let $q = 2^{t-2} + 2^{t-3} + 2^{l+2} - 5 = 2^{t-2} + 2^{t-3} + 4r - 1$.
Claim: $\binom{nr-1}{q} \equiv 8 \pmod{16}$.
Proof of claim: Let $\alpha(n)$ denote the number of 1's in the dyadic expansion of n.
Writing $nr - 1 = 2^t(2^l - 1) + 2^{l+2} - 5$, since $t > l+1$ we see that
$\alpha(nr-1) = \alpha(2^t(2^l-1)) + \alpha(4(2^l-1)-1) = 2l+1$.

Similarly, since $t - 3 > l + 1$, we get
$\alpha(q) = \alpha(2^{t-2} + 2^{t-3}) + \alpha((2^{l+2}-1)-4) = l+3$,
$\alpha(nr-1-q) = \alpha(2^{t+l} - 2^t - 2^{t-2} - 2^{t-3}) = l+1$.

Using Kummer's theorem $\nu_2(\binom{a}{b}) = \alpha(a-b) + \alpha(b) - \alpha(a)$, we see that $\nu_2(\binom{nr-1}{q}) = 3$ and the claim follows.

From the above claim we see that $(-1)^q\binom{nr-1}{q} \equiv 8 \pmod{16}$ is not a quadratic residue in $\mathbb{Z}/16\mathbb{Z}$. Since $n - 2q > 4$, it follows that $(-1)^q\binom{nr-1}{q}$ is a quadratic non-residue mod 2^{n-2q}. Invoking Theorem 1.1 completes the proof for the upper bound, while a straightforward computation (using [17]) of $k_{n,r}$ gives the lower bound. □

We remark that for $t = l+5 \geq 7$, the above example yields the following somewhat striking corollary.

Corollary 4.4. *Let* $t \geq 7$ *and* $d = d_{2^t+4,2^{t-5}-1} = (2^t+4)(2^{t-5}-1) - 2^{2t-11} + 2^{t-6}$. *Then* $d - 2^t \leq \operatorname{span}(X_{2^t+4,2^{t-5}-1}) \leq d - 2^t + 8$.

5 Appendix

The purpose of this appendix is to obtain a criterion, which is well-known to number theorists, for a given integer to be a quadratic residue in $\mathbb{Z}/p^n\mathbb{Z}$, where p a prime. Although our main interest is the case $p = 2$, we give the results for odd primes as well for the sake of completeness (Theorem 5.2) and add an elementary but probably new explicit result (Proposition 5.4) for $p = 2$.

We begin with the following lemma whose proof is left to the reader as an easy exercise.

Lemma 5.1. *Let p be any prime and $n \geq 1$. Let $a = p^k b$, $(p, b) = 1$, $1 \leq k < n$, be a quadratic residue mod p^n. Then k is even and b is a quadratic residue mod p^{n-k}.* $\square$

In view of the above lemma the discussion of when a given integer a is a quadratic residue mod p^n is reduced the case where $(a, p) = 1$. In the following, $(\mathbb{Z}/q\mathbb{Z})^*$ denotes the multiplicative group of units in the ring $\mathbb{Z}/q\mathbb{Z}$.

Theorem 5.2. *Let p be a prime and let $a \in \mathbb{Z}$ be prime to p. Let $n \geq 1$.*
(i) Let p be odd. Then a is a quadratic residue mod p^n if and only if it is so mod p.
(ii) Let $n \geq 3$. Then a is a quadratic residue mod 2^n if and only if $a \equiv 1$ (mod 8).

Proof:

(i) It is known that for any odd prime p, the group $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic of order $\varphi(p^n) = p^{n-1}(p-1)$. (See Ex. 2, p. 40, [12]), where φ denotes the Euler φ- function. The kernel K of the surjection $(\mathbb{Z}/p^n\mathbb{Z})^* \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^*$ has order p^{n-1}. Thus K is cyclic of odd order, whence any element in K is trivially a quadratic residue. It follows that an element of $\mathbb{Z}^*_{p^n}$ is a quadratic residue if and only if its image in $\mathbb{Z}^*_p$ is.
(ii) When $n \geq 3$, $(\mathbb{Z}/2^n\mathbb{Z})^*$ is *not* cyclic. However, it can be shown that the kernel K of the surjection $\mu : (\mathbb{Z}/2^n\mathbb{Z})^* \twoheadrightarrow (\mathbb{Z}/4\mathbb{Z})^*$ is cyclic of order 2^{n-2}, generated by $5 \in \mathbb{Z}/2^n\mathbb{Z}$ (Ex. 2, p. 40, [12]).

Factoring μ as the composition

$$(\mathbb{Z}/2^n\mathbb{Z})^* \overset{\lambda}{\twoheadrightarrow} (\mathbb{Z}/8\mathbb{Z})^* \twoheadrightarrow (\mathbb{Z}/4\mathbb{Z})^* ,$$

and noting that $1 \in (\mathbb{Z}/8)^*$ is the only quadratic residue there, we see that if $a \in (\mathbb{Z}/2^n\mathbb{Z})^*$ is a quadratic residue then $\lambda(a) = 1$, i.e. $a \equiv 1 \pmod 8$. Conversely, if $a \equiv 1 \pmod 8$, then $a \in \mathrm{Ker}\lambda \subset \mathrm{Ker}\mu = K$ implies $a \equiv 5^t \in K$ for some natural number t. But $\lambda(a) = 1$ then implies t is even, whence a is a quadratic residue. □

Remark 5.3. The reader is referred to [20] for generalizations and further information concerning quadratic residues. The next proposition generalizes Theorem 5.2 (ii) and gives explicitly all quadratic residues for $p = 2$. This result does not seem to appear in the literature, but the proof (given Theorem 5.2 (ii)) is fairly straightforward and is omitted.

Proposition 5.4. *(R.Scheidler) Let $n > 0$ and $a = 2^k b$ with b odd. For the equation $x^2 = a$ in $\mathbb{Z}/2^n\mathbb{Z}$, there is always a (trivial) solution for $n \leq k$ and no solution for $n > k$ with k odd. Assuming then that $n > k$ and k is even,*
(i) if $n = k+1$ there is always a solution,
(ii) if $n = k+2$ there is a solution if and only if $b \equiv 1 \pmod 4$,
(iii) if $n \geq k+3$ there is a solution if and only if $b \equiv 1 \pmod 8$. □

The final proposition is easily proved by induction, starting with $n = 4$, and using Theorem 5.2 (ii).

Proposition 5.5. *The number of quadratic residues in $\mathbb{Z}/2^n\mathbb{Z}$ is at most $2^n/4$, for $n \geq 4$.* □

References

[1] J.F.ADAMS, *Vector fields on spheres*, Ann. Math.**75**(1962), 603-632.

[2] E. ANTONIANO, *La accion del algebra de Steenrod sobre las variedades de Stiefel proyectivas*, Bol. Soc. Mat. Mexicana **22** (1977), 41-47.

[3] E.ANTONIANO, S.GITLER, J.UCCI, P.ZVENGROWSKI,*On the K-theory and parallelizability of projective Stiefel manifolds*, Bol. Soc. Mat. Mex. **31** (1986), 29-46.

[4] L.ASTEY, S.GITLER, E.MICHA, G.PASTOR, *Cohomology of complex projective Stiefel manifolds*, Can. J. Math. **51**, No.5 (1999), 897-914.

[5] L.ASTEY, S.GITLER, E.MICHA, G.PASTOR, *Parallelizability of complex projective Stiefel manifolds*, Proc. Amer. Math. Soc. **128**, No.5 (2000), 1527-1530.

[6] N.BARUFATTI, *Obstructions to immersions of projective Stiefel manifolds*, Differential topology, foliations, and group actions, Rio de Janeiro (1992), Contemp. Math. AMS **161** (1994), 281-287.

[7] N.BARUFATTI, D.HACON, *K-theory of projective Stiefel manifolds*, Trans. Amer. Math. Soc. **352** (2000), 3189-3209.

[8] N.BARUFATTI, D.HACON, K.Y.LAM, P.SANKARAN, P.ZVENGROWSKI, *The order of real line bundles*, Bol. Soc. Mat. Mex. (3) **10** (2004), 149-158.

[9] S.GITLER, D.HANDEL, *The projective Stiefel manifolds - I*, Topology **7** (1968), 39-46.

[10] S.GITLER,*The projective Stiefel manifolds - II. Applications*, Topology **7** (1968), 47-53.

[11] S.GITLER, K.Y.LAM, The K-theory of Stiefel Manifolds, Lect. Notes in Math.**168** (1970), Springer-Verlag, Berlin.

[12] N.KOBLITZ, A First Course on Number Theory and Cryptography, 2nd Ed., Springer-Verlag, Berlin, 1994.

[13] J.KORBAŠ, P.SANKARAN, P.ZVENGROWSKI, *Span of projective Stiefel manifolds*, Yellow Series (preprint)**704** (1991), Univ. of Calgary, Calgary, Canada.

[14] J.KORBAŠ, P.ZVENGROWSKI, *The vector field problem: a survey with emphasis on specific manifolds*, Expos. Math.**12** (1994), 3-20.

[15] J.KORBAŠ, P.ZVENGROWSKI, *On sectioning tangent bundles and other vector bundles*, Rend. del Circ. Mat. di Palermo Serie II, Suppl. 39 (1996), 85-104.

[16] K.Y.LAM, *A formula for the tangent bundle of flag manifolds and other related manifolds*, Trans. Amer. Math. Soc. **213** (1975), 343-350.

[17] K.Y.LAM, *Sectioning vector bundles over real projective spaces*, Quart. J. Math. Oxford (2) **23** (1972), 97-106.

[18] K.Y.LAM, D.RANDALL, *Geometric dimension of bundles on real projective spaces*, Contemp. Math. **188** (1995), 137-160.

[19] A.ROUX, *Application de la suite spectrale d'Hodgkin au calcul de la K-théorie des varietés de Stiefel*, Bull. Soc. Math. Fr. **99** (1971), 345-368.

[20] J.-P. SERRE, A Course in Arithmetic, GTM-**7**, Springer-Verlag, Berlin, 1973.

[21] L.SMITH, *Some remarks on projective Stiefel manifolds, immersions of projective spaces, and spheres*, Proc. Amer. Math. Soc.**80** (1980), 663-669.

[22] P.ZVENGROWSKI, *Recent progress in the topology of projective Stiefel manifolds*, Proc. 10th Brazilian Topology Meeting (Saõ Carlos, 1996), Mat. Contemp. **13**, (1997), 289-297.

[23] P.ZVENGROWSKI, *Remarks on the span of projective Stiefel manifolds*, Proc. 11th Brazilian Topology Meeting (Rio Claro, 1998), World Scientific, Singapore (2000), 85-98.