A Collection of
MTA–ELTE GAC manuscripts

Szabolcs L. Fancsali, Péter Sziklai

Higgledy-piggledy subspaces and uniform subspace designs

2016

MTA–ELTE Geometric and Algebraic
Combinatorics Research Group

Hungarian Academy of Sciences
Eötvös University, Budapest

MANUSCRIPTS
Higgledy-piggledy subspaces and uniform subspace designs

Szabolcs L. Fancsali*
MTA–ELTE Geometric and Algebraic Combinatorics Research Group
Budapest, Hungary
nudniq@cs.elte.hu

Péter Sziklai**
MTA–ELTE Geometric and Algebraic Combinatorics Research Group
ELTE, Institute of Mathematics, Department of Computer Science
Budapest, Hungary
sziklai@cs.elte.hu

January 5, 2016
Mathematics Subject Classifications: 05B25, 51E20, 51D20
keywords: projective space, subspace design, general position

Abstract
In this article, we investigate collections of ‘well-spread-out’ projective (and linear) subspaces. Projective $k$-subspaces in $\text{PG}(d,\mathbb{F})$ are in ‘higgledy-piggledy arrangement’ if they meet each projective subspace of co-dimension $k$ in a generator set of points. We prove that the set $\mathcal{H}$ of higgledy-piggledy $k$-subspaces has to contain more than $\min \left\{ |\mathbb{F}|, \sum_{i=0}^{k} \frac{d-k+i}{i+1} \right\}$ elements. We also prove that $\mathcal{H}$ has to contain more than $(k+1) \cdot (d-k)$ elements if the field $\mathbb{F}$ is algebraically closed.

---

*This research was partially supported by the ECOST Action IC1104 and OTKA Grant K81310

**This research was partially supported by the Bolyai Grant and OTKA Grant K81310
An r-uniform weak \((s,A)\) subspace design is a set of linear subspaces \(H_1, \ldots, H_N \subseteq \mathbb{F}^m\) each of rank \(r\) such that each linear subspace \(W \subseteq \mathbb{F}^m\) of rank \(s\) meets at most \(A\) among them. This subspace design is an \(r\)-uniform strong \((s,A)\) subspace design if \(\sum_{i=1}^{N} \text{rank}(H_i \cap W) \leq A\) for all \(W \subseteq \mathbb{F}^m\) of rank \(s\). We prove that if \(m = r + s\) then the dual \(\{(H_1^⊥, \ldots, H_N^⊥)\}\) of an \(r\)-uniform weak (strong) subspace design of parameter \((s,A)\) is an \(s\)-uniform weak (strong) subspace design of parameter \((r,A)\). We show the connection between uniform weak subspace designs and higgledy-piggledy subspaces proving that \(A \geq \min \{ |G|, \sum_{i=0}^{r-1} \binom{n+i}{i+1} \}\) for \(r\)-uniform weak or strong \((s,A)\) subspace designs in \(\mathbb{F}^{r+s}\).

We show that the \(r\)-uniform strong \((s, r \cdot s + \binom{d}{2})\) subspace design constructed by Guruswami and Kopparty (based on multiplicity codes) has parameter \(A = r \cdot s\) if we consider it as a weak subspace design. We give some similar constructions of weak and strong subspace designs (and higgledy-piggledy subspaces) and prove that the lower bound \((k+1) \cdot (d-k) + 1\) over algebraically closed field is tight.

1 Introduction

In our previous article [3], we examined sets \(G\) of points such that each hyperplane \(\Pi\) is spanned by the intersection \(\Pi \cap G\). Examination this question had been inspired by Héger, Patkós and Takáts [9], who hunt for a set \(G\) of points in the projective space \(\text{PG}(d,q)\) that ‘determines’ all hyperplanes in the sense that the intersection \(\Pi \cap G\) is unique for each hyperplane \(\Pi\).

A similar question is to find a set \(G\) of points such that each subspace \(\Pi\) of co-dimension \(k\) is spanned by the intersection \(\Pi \cap G\).

Recall that the lattice of projective subspaces of the projective geometry \(\text{PG}(d,F)\) can be considered as the lattice of linear subspaces of the vector space \(\mathbb{F}^{d+1}\). Each projective subspace \(\Pi \subseteq \text{PG}(d,F)\) of dimension \(k\) is actually a linear subspace of rank \(k+1\) in the vector space \(\mathbb{F}^{d+1}\), and each linear subspace \(W \subseteq \mathbb{F}^n\) of rank \(r\) is a projective subspace of dimension \(r-1\) in \(\text{PG}(n-1,F)\). If the field \(F\) is finite, we use the notation \(\text{PG}(d,q) = \text{PG}(d,\mathbb{F}_q)\).

For the sake of conciseness, a projective subspace of dimension \(k\) will be called a projective \(k\)-subspace and a subspace of co-dimension \(k\) will be called a \(k\)-subspace from now on.

Definition 1 (Multiple \(k\)-blocking set). A set \(B\) of points in the projective
space $\mathcal{P}G(d, \mathbb{F})$ is a $t$-fold blocking set with respect to co-$k$-subspaces (briefly, a $t$-fold $k$-blocking set), if each projective subspace $\Pi < \mathcal{P}G(d, \mathbb{F})$ of co-dimension $k$ meets $\mathcal{B}$ in at least $t$ points. A $t$-fold one-blocking set (i.e. with respect to hyperplanes) is briefly said to be a $t$-fold blocking set.

If $k > 1$ then the definition of the $t$-fold $k$-blocking set does not say anything more about the intersections with the co-$k$-subspaces. In higher dimensions, a natural specialization of multiple $k$-blocking sets would be the following.

**Definition 2** ($k$-generator set). A set $\mathcal{G}$ of points in the projective space $\mathcal{P}G(d, \mathbb{F})$ is a generator set with respect to co-$k$-subspaces (or briefly, a $k$-generator set), if each subspace $\Pi \subset \mathcal{P}G(d, \mathbb{F})$ of co-dimension $k$ meets $\mathcal{G}$ in a ‘generator system’ of $\Pi$, that is, $\mathcal{G} \cap \Pi$ spans $\Pi$, in other words this intersection is not contained in any hyperplane of $\Pi$. (Hyperplanes of co-$k$-subspaces are subspaces in $\mathcal{P}G(d, \mathbb{F})$ of co-dimension $k + 1$.)

If the field $\mathbb{F}$ is finite then a $k$-generator set of points is finite, and so we can ask the minimal cardinality of a $k$-generator set as a combinatorial question. Since finitely many points could generate only finitely many subspaces, a $k$-generator set of points must be infinite if the field $\mathbb{F}$ is not finite. But it could be the union of finitely many geometric objects. Such type of $k$-generator sets will be investigated in the following sections. Thus, we have combinatorial questions over arbitrary fields.

### 1.1 Higgledy-piggledy subspaces

Héger, Patkós and Takáts [9] had the idea to search for generator sets with respect to hyperplanes as the union of some disjoint projective lines. The generalization of this idea is to search for generator sets with respect to co-$k$-subspaces as the union of some (possibly disjoint) projective $k$-spaces. Note that the union of $t$ disjoint projective $k$-spaces is always a $t$-fold $k$-blocking set.

**Definition 3** (Higgledy-piggledy $k$-subspaces). Let $\mathcal{H}$ be a set of projective $k$-subspaces. If the set $\bigcup \mathcal{H}$ of all points of the subspaces contained by $\mathcal{H}$ is a generator set with respect to co-$k$-subspaces, then the elements of $\mathcal{H}$ is said to be in higgledy-piggledy arrangement and the set $\mathcal{H}$ itself is said to be a set of higgledy-piggledy $k$-subspaces.
The terminology ‘higgledy-piggledy arrangement’ is introduced by Héger, Patkós and Takáts [9] in the case of ‘higgledy-piggledy lines’.

At first, we try to give another equivalent definition to the ‘higgledy-piggledy’ property of sets of $k$-subspaces. The following is not an equivalent but a sufficient condition. Although, in several cases it is also a necessary condition (if we seek minimal such sets), thus, it could effectively be considered as an almost-equivalent.

**Theorem 4** (Sufficient condition). If there is no subspace of co-dimension $k + 1$ meeting each element of the set $\mathcal{H}$ of $k$-subspaces then $\mathcal{H}$ is a set of higgledy-piggledy $k$-subspaces.

**Proof.** Suppose that the set $\bigcup \mathcal{H}$ is not a generator set with respect to co-$k$-subspaces. Then there exists at least one co-$k$-subspace $\Pi$ that meets $\bigcup \mathcal{H}$ in a set $\Pi \cap (\bigcup \mathcal{H})$ of points which is contained in a hyperplane $W$ of $\Pi$. Since $\Pi$ is of co-dimension $k$ it meets every projective $k$-subspace, thus each element of $\mathcal{H}$ meets $\Pi$, but the point(s) of intersection has (have) to be contained in $W$. Thus the subspace $W$ (of co-dimension $k + 1$) meets each element of $\mathcal{H}$.

Chistov et. al in [1] and in [2] called a finite family $\mathcal{H}$ of rank-$r$ linear subspaces of $\mathbb{F}^n$ having property $\mathcal{P}_{n,r}(\mathbb{F})$ iff for every linear subspace $W \leq \mathbb{F}^n$ of rank $(n - r)$ there exists at least one element $H \in \mathcal{H}$ which is transversal to $W$, that is, $H$ and $W$ are disjoint projective subspaces of $\text{PG}(n - 1, \mathbb{F})$. So the finite family $\mathcal{H}$ of $(r - 1)$-dimensional projective subspaces of $\text{PG}(n - 1, \mathbb{F})$ has property $\mathcal{P}_{n,r}(\mathbb{F})$ if and only if there is no projective subspace $W$ of dimension $(n - r - 1)$ (co-dimension $r$) that meets each element of $\mathcal{H}$.

The theorem above says that every finite family $\mathcal{H}$ of $k$-dimensional projective subspaces of $\text{PG}(d, \mathbb{F})$ having property $\mathcal{P}_{d+1,k+1}(\mathbb{F})$ is a set of higgledy-piggledy $k$-subspaces. The theorem above is a sufficient but not necessary condition. But if this condition above does not hold, then the set $\mathcal{H}$ of $k$-subspaces could only be a set of higgledy-piggledy $k$-subspaces in a very special way.

**Proposition 5.** If the set $\mathcal{H}$ of $k$-subspaces of $\text{PG}(d, \mathbb{F})$ is set of higgledy-piggledy $k$-subspaces and there exists a subspace $W$ of co-dimension $k + 1$ that meets each element of $\mathcal{H}$ then $\mathcal{H}$ has to contain at least as many elements as many points there are in a projective line. (That is, $|\mathcal{H}| \geq q + 1$ if the field $\mathbb{F} = \mathbb{F}_q$ and $\mathcal{H}$ is infinite if the field $\mathbb{F}$ is not finite.)
Proof. The points of the factor geometry $\PG(d, \mathbb{F})/W \cong \PG(k, \mathbb{F})$ are the co-$k$-subspaces of $\PG(d, \mathbb{F})$ containing $W$. Let $H_i \in \mathcal{H}$ a $k$-subspace and consider the projective subspace $H_i \vee W$ spanned by $H_i$ and $W$. Since $W$ meets $H_i$, $H_i \vee W$ could not be the whole projective space. By factorization with $W$, $H_i \vee W$ becomes a proper projective subspace or the emptyset. A point $P$ of the factor geometry $\PG(d, \mathbb{F})/W \cong \PG(k, \mathbb{F})$ as a co-$k$-subspace $\hat{P}$ of $\PG(d, \mathbb{F})$ could only be generated by $\mathcal{H}$ only if there exists a $k$-subspace $H_i \in \mathcal{H}$ such that $\hat{P} \cap H_i$ is not contained in $W$, that is, $H_i \vee W$ as a subspace (of the factor geometry) contains $P$. Thus, if $\mathcal{H}$ is a set of higgledy-piggledy $k$-subspaces, and $\mathcal{H}$ is blocked by the subspace $W$ of co-dimension $k+1$, then $\mathcal{H}$ is a set of proper subspaces of the factor geometry $\PG(d, \mathbb{F})/W \cong \PG(k, \mathbb{F})$, covering all points of this projective space.

Extending these proper subspaces to hyperplanes of the factor geometry, and then consider these hyperplanes as the points of the dual geometry $(\PG(d, \mathbb{F})/W)^*$, we have a blocking set with respect to hyperplanes of $(\PG(d, \mathbb{F})/W)^*$, thus, it has to contain at least as many elements as many points there are in a projective line.

**Corollary 6.** Suppose that the set $\mathcal{H}$ of $k$-subspaces has at most $|\mathbb{F}|$ elements. Then $\mathcal{H}$ is a set of higgledy-piggledy $k$-subspaces if and only if there is no subspace of co-dimension $k+1$ meeting each element of $\mathcal{H}$.

Thus, the sufficient condition in Theorem 4 is an equivalent condition if $|\mathcal{H}| \leq |\mathbb{F}|$, that’s why we called it ‘almost-equivalent’.

**Remark 7.** If $\mathcal{H}$ is a set of (much more than $N$) projective $k$-subspaces such that there is no subspace $W$ of co-dimension $k+1$ meeting at least $N$ elements of $\mathcal{H}$ then arbitrary $N$ elements of $\mathcal{H}$ are in higgledy-piggledy arrangement.

### 1.2 Uniform weak subspace designs

A similar (but not identical) property is called ‘well-spread-out’ by Guruswami and Kopparty in [8] where they gave the definition [8, Definition 2] of weak $(s, A)$ subspace designs. Since we are interested in subspace designs containing subspaces of the same dimension, we define the notion of a uniform subspace design. From now on, we use the word rank in linear context and the word dimension in projective context exclusively, to avoid confusion.

**Definition 8** (Uniform weak subspace design). A collection $\{H_1, \ldots, H_N\}$ of linear subspaces of rank $r$ in the vector space $\mathbb{F}^m$ is called an $r$-uniform...
weak \((s, A)\) subspace design if for every linear subspace \(W \subset \mathbb{F}^m\) of rank \(s\), the number of indices \(i\) for which \(\text{rank}(H_i \cap W) > 0\) is at most \(A\).

This definition is nontrivial only if the subspace design contains at least \(N \geq A + 1\) subspaces. Since a linear subspace \(W\) of rank \(s\) and a linear subspace \(H\) of rank \(r\) always meet each other nontrivially in the vector space \(\mathbb{F}^m\) if \(s + r > m\), the parameter \(r\) should be at most \(m - s\) if we seek nontrivial \(r\)-uniform \((s, A)\) subspace designs.

The standard scalar product \(\langle a \mid b \rangle = \sum_{i=0}^{m-1} a_i b_i\) makes the isomorphism \((\mathbb{F}^m)^* \equiv \mathbb{F}^m\) canonical, in other words, the vector space \(\mathbb{F}^m\) is self-dual. Let \(H^+ = \{a \in (\mathbb{F}^m)^* \mid \langle a \mid b \rangle = 0 : \forall b \in H\}\) denote the annihilator (orthogonal complementary) subspace of \(H \leq \mathbb{F}^m\) in \((\mathbb{F}^m)^* \equiv \mathbb{F}^m\). If rank \(H = r\) then rank \(H^+ = m - r\).

If the parameter \(r\) equals to \(m - s\), then the dual of an \(r\)-uniform subspace design \(\mathcal{H}\) (containing the annihilators of the elements of \(\mathcal{H}\)) is again a uniform subspace design.

**Theorem 9.** If \(\{H_1, \ldots, H_N\}\) is an \((m - s)\)-uniform weak \((s, A)\) subspace design in the linear space \(\mathbb{F}^m\) of rank \(m\) then the collection \(\{H_1^+, \ldots, H_N^+\}\) of co-(\(m - s\))-subspaces in the dual vector space \((\mathbb{F}^m)^*\) is an \(s\)-uniform weak \((m - s, A)\) subspace design.

**Proof.** The linear subspace \(W\) of rank \(s\) and a linear subspace \(H\) of rank \(m - s\) meet each other nontrivially in the vector space \(\mathbb{F}^m\) if and only if there exists a hyperplane \(\Pi\) containing both \(H\) and \(W\). In the dual space \((\mathbb{F}^m)^*\) it means that the one-dimensional subspace \(\Pi^\perp\) is contained by both \(H^\perp\) and \(W^\perp\).

If the parameter \(r\) is less than \(m - s\) then the dual of an \(r\)-uniform \((s, A)\) subspace design in the linear space \(\mathbb{F}^m\) is not necessarily a nontrivial subspace design.

If the weak \((s, A)\) subspace design \(\mathcal{H} = \{H_1, \ldots, H_N\}\) is non-uniform (that is, for each linear subspace \(W \prec \mathbb{F}^m\) of rank \(s\) there exist at most \(A\) elements of \(\mathcal{H}\) meeting \(W\) non-trivially but for example rank \(H_1 \neq \text{rank} H_2\) then its dual is not necessarily a weak subspace design at all.

The following proposition makes connection between uniform weak subspace designs and higgledy-piggledy subspaces.

**Proposition 10.** If the set \(\{H_1, \ldots, H_N\}\) of linear subspaces is a \((k+1)\)-uniform weak \((d-k, A)\) subspace design in the vector space \(\mathbb{F}^{d+1}\) then arbitrary
subset $\mathcal{H}$ of at least $A+1$ elements (among $H_1, \ldots, H_N$) is a set of projective $k$-subspaces in higgledy-piggledy arrangement.

And conversely, suppose that $\{H_1, \ldots, H_N\}$ is a set of projective $k$-subspaces in $\mathbb{P}G(d, \mathbb{F})$ and there exists a finite positive integer $A < |\mathbb{F}|$ such that for each subset $\mathcal{H} \subset \{H_1, \ldots, H_N\}$: if $|\mathcal{H}| = A+1$ then $\mathcal{H}$ is a set of $k$-subspaces in higgledy-piggledy arrangement. In this case $\{H_1, \ldots, H_N\}$ is a set of linear subspaces constituting a $(k+1)$-uniform weak $(d-k, A)$ subspace design in the vector space $\mathbb{F}^{d+1}$.

Proof. If $\{H_1, \ldots, H_N\}$ is a $(k+1)$-uniform weak $(d-k, A)$ subspace design in $\mathbb{F}^{d+1}$ and $\mathcal{H}$ is a subset of at least $A+1$ elements among $H_1, \ldots, H_N$ then for each linear subspace $W < \mathbb{F}^{d+1}$ of rank $d-k$ (i.e. $W < \mathbb{P}G(d, \mathbb{F})$ is of co-dimension $k+1$) there exists at least one element of $\mathcal{H}$ disjoint to $W$ in projective sense (or meeting $W$ trivially in linear sense). So, $\mathcal{H}$ satisfies the sufficient condition of Theorem 4.

Suppose that each subset $\mathcal{H} \subset \{H_1, \ldots, H_N\}$ of cardinality $A+1$ is a set of projective $k$-subspaces in higgledy-piggledy arrangement. Since $A$ is less then the cardinality of the field $\mathbb{F}$, then $|\mathcal{H}| = A+1$ is less than the cardinality of a projective line, and thus, Proposition 5 concludes that there cannot exist a projective subspace $W$ of co-dimension $k+1$ (i.e. a linear subspace of rank $d-k$) meeting each element of $\mathcal{H}$. Thus, for each linear subspace $W$ of rank $d-k$ there are at most $A$ elements of $\{H_1, \ldots, H_N\}$ meeting $W$ nontrivially.

In other words, each subset $\mathcal{H}$ of a $(k+1)$-uniform weak $(d-k, A)$ subspace design (in $\mathbb{F}^{d+1}$) has property $\mathcal{P}_{d+1,k+1}(\mathbb{F})$ if $|\mathcal{H}| \geq A+1$. And conversely, let $\mathcal{F}$ be a family of rank-$(k+1)$ linear subspaces of $\mathbb{F}^{d+1}$. If each subset $\mathcal{H} \subseteq \mathcal{F}$ of cardinality bigger than $A$ has property $\mathcal{P}_{d+1,k+1}(\mathbb{F})$ then $\mathcal{F}$ is a $(k+1)$-uniform weak $(d-k, A)$ subspace design.

### 1.3 Uniform strong subspace designs

Guruswami and Kopparty defined the strong $(s, A)$ subspace designs in [8, Definition 3]. One can define a uniform variant of strong subspace designs (containing same rank subspaces) as follows.

**Definition 11** (Uniform strong subspace design). A collection $\{H_1, \ldots, H_M\}$ of linear subspaces of rank $r$ in the vector space $\mathbb{F}^m$ is called an $r$-uniform
strong \((s,A)\) subspace design if for every linear subspace \(W \subset \mathbb{F}^m\) of rank \(s\), the sum \(\sum_{i=1}^{M} \text{rank}(H_i \cap W)\) is at most \(A\).

Remark 12. As mentioned also by Guruswami and Kopparty [8], every \(r\)-uniform strong \((s,A)\) subspace design is also an \(r\)-uniform weak \((s,A)\) subspace design, and every \(r\)-uniform weak \((s,A)\) subspace design is also an \(r\)-uniform strong \(\{sA, rA\}\) subspace design.

Guruswami and Kopparty [8] constructed \(r\)-uniform strong \((s,A)\) subspace designs in the vector space \(\mathbb{F}_q^m\) over the finite field of \(q > m\) elements. Their first construction [8, Section 4] is based on Reed–Solomon codes. Their second construction [8, Section 5] is based on multiplicity codes but this second construction works only if \(\text{char } \mathbb{F}_q > m\). Translating the notation of Guruswami’s and Kopparty’s work [8] to the slightly different convention of this article, [8, Theorem 14, Theorem 17 and Theorem 20] say that \(A \leq \frac{(m-1)s}{m-r-h(s-1)}\) for both constructions. The work [3] sharpened these results as follows.

Theorem 13 ([3, Theorem 38]). \(A \leq \frac{(m-2)s}{m-r-h(s-1)}\) for the first Guruswami–Kopparty construction, and \(A \leq \frac{(m-s)s}{m-r-h(s-1)}\) for the second Guruswami–Kopparty construction. \(\square\)

Remark 14. The parameter what we denote here \(h\), comes from the trick of applying the extension field \(\mathbb{F}_{q^s}\) during the constructions. The basic case is \(h = 1\). The constraint \(m - r > h (s - 1)\) results in the bound of \(\frac{m-r}{s-1} > h > 0\) if \(s > 1\).

Theorem 15. The dual of a \((m-s)\)-uniform strong \((s,A)\) subspace design in \(\mathbb{F}^m\) is an \(s\)-uniform strong \((m-s,A)\) subspace design in \((\mathbb{F}^m)^* \equiv \mathbb{F}^m\).

Proof. Let the set \(\{H_1, \ldots, H_N\}\) of linear subspaces \(H_i \subset \mathbb{F}^m\), \(\text{rank } H_i = m - s\) be a uniform strong \((s, A)\) subspace design, that is, for each linear subspace \(W \subset \mathbb{F}^m\) of rank \(s\), \(\sum_{i=1}^{N} \text{rank}(W \cap H_i) \leq A\).

Then the linear subspaces \(H_1^\perp, \ldots, H_N^\perp\) in \((\mathbb{F}^m)^* \equiv \mathbb{F}^m\) are of rank \(s\) and for each linear subspace \(V \subset (\mathbb{F}^m)^*\) of rank \(m-s\) there exists a linear subspace \(W \subset \mathbb{F}^m\) of rank \(s\) such that \(V = W^\perp\).

We know that \(\text{rank } V^\perp = m - \text{rank } V\) and \((W \lor H_i)^\perp = W^\perp \cap H_i^\perp\), thus, \(m - \text{rank}(W \lor H_i) = \text{rank}(W \lor H_i^\perp) = \text{rank}(W^\perp \cap H_i^\perp)\).

Since \(\text{rank}(W \cap H_i) = \text{rank } W + \text{rank } H_i - \text{rank}(W \lor H_i) = s + (m - s) - \text{rank}(W \lor H_i) = m - \text{rank}(W \lor H_i) = \text{rank}(W^\perp \cap H_i^\perp)\) then the sum

\[\text{rank}(W \cap H_i) = \text{rank}(W^\perp \cap H_i^\perp)\]
$$\sum_{i=1}^{N} \text{rank}(W_i \cap H_i) = \sum_{i=1}^{N} \text{rank}(W \cap H_i) \leq A$$ for each linear subspace 
$$W_i \perp (\mathbb{F}^m)^*$$ of rank \(m - s\).

In this article, we are interested in \(r\)-uniform strong or weak \((s, A)\) subspace designs in \(\mathbb{F}^m\) where \(r + s = m\). If \(s > 1\) (and \(m = r + s\)) then the bound \(\frac{r\cdot s}{r-1} > h > 0\) has the form \(1 + \frac{1}{r-1} = \frac{s}{r-1} > h > 0\), thus, in this case \(h = 1\) is required in the Guruswami–Kopparty constructions. Thus, the first Guruswami–Kopparty construction gives us an \(r\)-uniform strong \((s, r\cdot s + \binom{s}{2})\) subspace design; and the second Guruswami–Kopparty construction (working if \(\text{char} \mathbb{F}_q > m = r + s\)) gives us an \(r\)-uniform strong \((s, r \cdot s)\) subspace design.

**Corollary 16.** For given \(s \geq 2\) and \(r \geq 2\) there exist an \(r\)-uniform strong 
\((s, r \cdot s + \min\{\binom{r}{2}, \binom{s}{2}\})\) subspace design in the vector space \(\mathbb{F}^{r+s}\) if the field \(\mathbb{F}\) has more than \(r + s\) elements. Moreover, for given \(s \geq 2\) and \(r \geq 2\) there exist an \(r\)-uniform strong \((s, r \cdot s)\) subspace design in the vector space \(\mathbb{F}^{r+s}\) if the characteristic \(\text{char} \mathbb{F}\) of the field \(\mathbb{F}\) is bigger than \(r + s\).

**Proof.** Theorem 15 above says that the duals of the first and second Guruswami–Kopparty constructions are \(s\)-uniform strong \((r, r \cdot s + \binom{s}{2})\) and \(s\)-uniform strong \((r, r \cdot s)\) subspace designs, respectively. The second construction works only if \(\text{char} \mathbb{F}_q > m = r + s\), but the first construction and its dual work over a field \(\mathbb{F}\) of arbitrary characteristic if \(\mathbb{F}\) has more than \(r + s\) elements.

The first Guruswami–Kopparty construction gives us an \(r\)-uniform strong \((s, r \cdot s + \binom{s}{2})\) subspace design and an \(s\)-uniform strong \((r, s \cdot r + \binom{r}{2})\) subspace design. The dual of this last design is an \(r\)-uniform strong \((s, s \cdot r + \binom{r}{2})\) subspace design.

### 1.4 Lower bound over arbitrary (large enough) fields

In this section we give lower bounds for the cardinality of a set of subspaces in higgledy-piggledy arrangement. In our previous work [3], we proved the following lemma.

**Lemma 17.** [3, Lemma 13] If the set \(\mathcal{L}\) of lines in \(\text{PG}(d, \mathbb{F})\) has at most \(\left\lfloor \frac{d}{2} \right\rfloor + d - 1\) elements then there exists a subspace \(H\) of co-dimension two meeting each line in \(\mathcal{L}\).

This lemma can be generalized by induction as follows.
Lemma 18. If the set $\mathcal{H}$ of $k$-subspaces in $\text{PG}(d, \mathbb{F})$ has at most $\left[ \frac{d}{k+1} \right] + \left[ \frac{d-1}{k} \right] + \cdots + \left[ \frac{d-k+1}{2} \right] + d - k$ elements then there exists a subspace $W$ of co-dimension $k + 1$ meeting each subspace in $\mathcal{H}$.

Proof. Suppose by induction that for each $m$, at most $\left[ \frac{m}{k} \right] + \left[ \frac{m-1}{k} \right] + \cdots + \left[ \frac{m-k+2}{2} \right] + m - (k - 1)$ subspaces of dimension $k - 1$ in $\text{PG}(m, \mathbb{F})$ always be blocked by a subspace $W$ of co-dimension $k$. Lemma 17 says that this base of induction holds for $k = 2$. Let $H_1, \ldots, H_{\frac{d}{k+1}}$ and $H_{\frac{d}{k+1}+1}$ (1 ≤ $i$ ≤ $\left[ \frac{d-1}{k} \right] + \cdots + \left[ \frac{d-k+1}{2} \right] + d - k$) denote the elements of $\mathcal{H}$. There exists a subspace of dimension at most $(k + 1) \left[ \frac{d}{k+1} \right] - 1$ containing the $k$-subspaces $H_1, \ldots, H_{\frac{d}{k+1}}$ so there exists a hyperplane $\Pi$ containing them. The hyperplane $\Pi$ meets each $k$-subspace in a subspace of dimension at least $k - 1$, thus let $L_i \leq \Pi \cap H_{\frac{d}{k+1}+1}$ be a $(k - 1)$-subspace for $i = 1, \ldots, \left[ \frac{m}{k} \right] + \left[ \frac{m-1}{k} \right] + \cdots + \left[ \frac{m-k+2}{2} \right] + m - (k - 1)$, where $m = d - 1$.

By induction there exists a subspace $W < \Pi$ of co-dimension $k$ (co-dimension with respect to $\Pi$), that meets each subspace $L_i$ above, so $W$ meets the subspaces $H_{\frac{d}{k+1}+1}$, 1 ≤ $i$ ≤ $\left[ \frac{d-1}{k} \right] + \left[ \frac{d-2}{k-1} \right] + \cdots + \left[ \frac{d-k+1}{2} \right] + d - k$. Subspaces $H_1, \ldots, H_{\frac{d}{k+1}}$ are contained in $\Pi$, and $W$ has co-dimension $k$ in $\Pi$, thus, $W$ meets them also. The subspace $W$ has co-dimension $k + 1$ in $\text{PG}(d, \mathbb{F})$ and it meets all the elements of $\mathcal{H}$. \hfill \Box

Corollary 19. So a family $\mathcal{H}$ of property $\mathcal{P}_{d+1,k+1}(\mathbb{F})$ has to contain at least $1 + \sum_{i=0}^{k} \left[ \frac{d-k+i}{k+1} \right]$ elements. \hfill \Box

Theorem 20 (Lower bound). A set $\mathcal{H}$ of higgedly-piggedly $k$-subspaces in $\text{PG}(d, \mathbb{F})$ has to contain at least $\min \left\{ |\mathbb{F}|, \sum_{i=0}^{k} \left[ \frac{d-k+i}{k+1} \right] \right\} + 1$ elements.

Proof. If there exists a projective subspace $W$ of co-dimension $k + 1$ meeting each element of $\mathcal{H}$ then Proposition 5 says that $|\mathcal{H}| > |\mathbb{F}|$.

If there does not exist any projective subspace $W$ of co-dimension $k + 1$ meeting each element of $\mathcal{H}$ then Lemma 18 gives the result. \hfill \Box

As a consequence of this lower bound we get a bound for the parameter $A$ of weak $r$-uniform $(s, A)$ subspace designs.

Corollary 21. If the field $\mathbb{F}$ has at least $\left[ \frac{m-1}{r} \right] + \left[ \frac{m-2}{r-1} \right] + \cdots + \left[ \frac{m-r+1}{2} \right] + m - r + 1$ elements, then for each $r$-uniform weak $(m - r, A)$ subspace design in $\mathbb{F}^m$, the parameter $A$ has to be at least $\left[ \frac{m-1}{r} \right] + \left[ \frac{m-2}{r-1} \right] + \cdots + \left[ \frac{m-r+1}{2} \right] + m - r$. 


Proof. Let \( d = m - 1 \) and \( k = r - 1 \). Proposition 10 says that arbitrary \( A + 1 \) elements of a \( (k + 1) \)-uniform weak \( (d - k, A) \) subspace design (in \( \mathbb{F}^{d+1} \)) are projective \( k \)-subspaces (of \( \mathbb{P}G(d, \mathbb{F}) \)) in higgledy-piggledy position. Theorem 20 concludes that \( A+1 \geq \left\lfloor \frac{d}{k+1} \right\rfloor + \left\lfloor \frac{d}{2k} \right\rfloor + \cdots + \left\lfloor \frac{d}{k+1} \right\rfloor + d-k+1. \)

\[ \Box \]

\section{Grassmann coordinates}

Let \( \mathbb{G}(r, s, \mathbb{F}) \) or simply \( \mathbb{G}(r, s) \) denote the Grassmannian of the linear subspaces of rank \( r \) (and so, of co-dimension \( s \)) in the vector space \( \mathbb{F}^{r+s} \), or, in other aspect \( \mathbb{G}(r, s) \) is the set of all projective subspaces of dimension \( r-1 \) (and co-dimension \( s \)) in \( \mathbb{P}G(r+s-1, \mathbb{F}) \).

\textbf{Plücker embedding} \quad \text{Let} \ H < \mathbb{F}^{r+s} \text{ be a linear subspace of rank } r \text{ and let } a(1), \ldots, a(r) \text{ and } b(1), \ldots, b(r) \text{ be two arbitrary bases of } H. \text{ Let } L < \mathbb{F}^{r+s} \text{ be another linear subspace of rank } r (H \neq L) \text{ and let } c(1), \ldots, c(r) \text{ be a basis of } L. \text{ Since } a(1) \wedge \cdots \wedge a(r) = \lambda \cdot b(1) \wedge \cdots \wedge b(r) \neq 0 \text{ for a suitable nonzero } \lambda \in \mathbb{F}, \text{ and since } c(1) \wedge \cdots \wedge c(r) \neq 0 \text{ is not the element of the subspace of rank one, generated by } a(1) \wedge \cdots \wedge a(r), \text{ this subspace } \{a(1) \wedge \cdots \wedge a(r) \cdot \lambda \mid \lambda \in \mathbb{F}\} < \bigwedge^r \mathbb{F}^{r+s} \text{ of rank one can be identified with } H. \text{ This \textquoteleft Plücker embedding\textquoteright identifies the Grassmannian with the set of rank-one linear subspaces of } \bigwedge^r \mathbb{F}^{r+s} \text{ generated by totally decomposable multivectors, that is, } \mathbb{G}(r, s) \subset \mathbb{P}G(\bigwedge^r \mathbb{F}^{r+s}) \equiv \mathbb{P}G((^{r+s}_r) - 1, \mathbb{F}) \text{ is an algebraic variety of dimension } r \cdot s.

\textbf{Grassmann coordinates} \quad \text{Let } H \in \bigwedge^r \mathbb{F}^{r+s} \text{ denote a homogeneous coordinate vector of a point in } \mathbb{P}G((^{r+s}_r) - 1, \mathbb{F}). \text{ If } H \in \bigwedge^r \mathbb{F}^{r+s} \text{ is nonzero and totally decomposable (i.e. } H = a(1) \wedge \cdots \wedge a(r) \neq 0) \text{ is a multivector for suitable vectors } a(i) \in \mathbb{F}^{r+s} \text{ then } H \text{ is called the \textquoteleft Grassmann coordinate vector\textquoteright of the subspace } H \text{ generated by the vectors } a(i) \in \mathbb{F}^{r+s}. \text{ The coordinates } H_{i_1 \ldots i_r} \in \mathbb{F} (0 \leq i_1, \ldots, i_r \leq r + s - 1) \text{ of the multivector } H \text{ are called the Grassmann coordinates of the subspace } H < \mathbb{F}^{r+s} \text{ of rank } r.

\textbf{Plücker relations} \quad \text{The numbers } H_{i_1 \ldots i_r} \in \mathbb{F} (0 \leq i_1 \ldots i_r \leq r + s - 1) \text{ are the coordinates of a totally decomposable multivector } H \text{ (i.e. the Grassmann coordinates of the subspace } H < \mathbb{F}^{r+s} \text{ if and only if for each } 2r\text{-tuple}
\((i_1, \ldots, i_{r-1}, j_0, j_1, \ldots, j_r)\) of indices (each of them between zero and \(r + s - 1\))

\[
\sum_{n=0}^{r} (-1)^n H_{i_1 \ldots i_{r-1} j_n} H_{j_0 \ldots j_n \ldots j_r} = 0 \tag{P1}
\]

where the notation \(j_0 \ldots j_n \ldots j_r\) means that the symbol \(j_n\) is missing from the list \(j_0 \ldots j_r\) of symbols. These quadratic equations are called ‘Plücker relations’ and according to [10, Theorem 3.1.6.], the Plücker relations completely determine the Grassmannian \(G(r, s) \subset PG\left(\binom{r+s}{s} - 1, \mathbb{F}\right)\), moreover, they generate the ideal of polynomials vanishing on it.

The following property of the Plücker relations will play a key role later.

**Lemma 22.** Consider the Grassmann coordinates of the elements of \(G(r, s)\) or \(G(s, r)\), and let \(N\) be a positive integer between \(r\) and \(r \cdot s\). Let the integers \(i_1, \ldots, i_r, j_0, j_1, \ldots, j_r\) be given such that \(i_1 + \cdots + i_r = N = j_1 + \cdots + j_r\) and \(0 \leq i_1 < \cdots < i_r \leq r + s - 1\) and \(0 \leq j_1 < \cdots < j_r \leq r + s - 1\) and suppose that \((i_1, \ldots, i_r) \neq (j_1, \ldots, j_r)\). Then there exists a Plücker relation that has the form

\[
H_{i_1 \ldots i_r} H_{j_1 \ldots j_r} + \Sigma = 0
\]

where \(\Sigma\) is the sum of some products \(H_{k_1 \ldots k_r} H_{n_1 \ldots n_r}\), where \(k_1 + \cdots + k_r < N < n_1 + \cdots + n_r\).

**Proof.** Since \((i_1, \ldots, i_r) \neq (j_1, \ldots, j_r)\), there exists an index \(i_\ell \notin \{j_1, \ldots, j_r\}\). There exists an even permutation \(\sigma \in S_r\) such that \(\sigma \ell = \ell\). The Plücker relation according to the 2r-tuple \((i_{\sigma 1} \ldots i_{\sigma (r-1)}, j_0 = i_{\sigma r}, j_1, \ldots, j_r)\) is

\[
H_{i_{\sigma 1} \ldots i_{\sigma r}} H_{j_1 \ldots j_r} + \sum_{n=1}^{r} (-1)^n H_{i_{\sigma 1} \ldots i_{\sigma (r-1)} j_n} H_{j_0 \ldots j_n \ldots j_r} = 0 \tag{P2}
\]

using the notation \(j_0 = i_{\sigma r} = i_\ell\) and separating the first term of the sum.

Because \(j_0 = i_\ell, j_1, \ldots, j_r\) are \(r + 1\) distinct elements, \(j_n\) is either strictly less or strictly greater than \(j_0\) if \(n \neq 0\), and thus, \((\sum_{k=0}^{r} j_k) - j_n\) is either strictly greater or strictly less than \(N = \sum_{k=1}^{r} j_k\) if \(n \neq 0\). And, since \(i_{\sigma 1} + \cdots + i_{\sigma (r-1)} + i_{\sigma r} + j_1 + \cdots + j_r = 2N\), if \((\sum_{k=0}^{r} j_k) - j_n > N\) then \(i_{\sigma 1} + \cdots + i_{\sigma (r-1)} + j_n < N\), and conversely, if \((\sum_{k=0}^{r} j_k) - j_n < N\) then \(i_{\sigma 1} + \cdots + i_{\sigma (r-1)} + j_n > N\).

And last, since \(\sigma\) is even, then \(H_{i_1 \ldots i_r} = H_{i_{\sigma 1} \ldots i_{\sigma r}}\), we get that the Plücker relation P2 is in the required form. \(\square\)

**Remark 23.** If \(\{i_1, \ldots, i_r\} = \{j_1, \ldots, j_r\}\) then each Plücker relation containing the product \(H_{i_1 \ldots i_r} H_{j_1 \ldots j_r}\) reduces to \(0 = 0\).
2.1 Dual Grassmann coordinates

Since the map \( \star : \mathbb{G}(s, r) \to \mathbb{G}(r, s) : W \mapsto W^\perp \) is a bijection between the linear subspaces of rank \( r \) and the linear subspaces of rank \( s \), we could define ‘dual’ Grassmann coordinates of rank-\( s \) subspaces having \( r \) indices instead of \( s \).

Let \( W < \mathbb{F}^{r+s} \) be an arbitrary subspace of rank \( s \) and let \( W^\perp < \mathbb{F}^{r+s} \) its orthogonal complementary subspace of rank \( r \). The Grassmann coordinate vector \( \mathbf{W}^* \) of the orthogonal complementary subspace \( W^\perp \) is called the ‘dual Grassmann coordinate vector’ of the subspace \( W \). The coordinates \( W_{i_1 \cdots i_r} \in \mathbb{F} \ (0 \leq i_1 \cdots i_r \leq r + s - 1) \) of the multivector \( \mathbf{W}^* \) are called the ‘dual Grassmann coordinates’ of the subspace \( W < \mathbb{F}^{r+s} \) of rank \( s \).

Although the Grassmann coordinate vector of the subspace \( W \) is denoted by \( \mathbf{W} \), the Grassmann coordinate vector of its orthogonal complementary subspace \( W^\perp \) is denoted by \( \mathbf{W}^* \) instead of \( \mathbf{W}^\perp \) because we want to avoid confusion between similar notations and the notation \( \{\mathbf{W}\}^\perp \) means the hyperplane of the vector space (\( \bigwedge^r \mathbb{F}^{r+s} \)*) orthogonal to the vector \( \mathbf{W} \in \bigwedge^s \mathbb{F}^{r+s} \).

The standard scalar product of the outer power space \( \bigwedge^r \mathbb{F}^{r+s} \) is defined by the following identity

\[
\langle a(1) \wedge \cdots \wedge a(r)|b(1) \wedge \cdots \wedge b(r)\rangle = \begin{vmatrix}
\langle a(1)|b(1)\rangle & \cdots & \langle a(1)|b(r)\rangle \\
\vdots & \ddots & \vdots \\
\langle a(r)|b(1)\rangle & \cdots & \langle a(r)|b(r)\rangle
\end{vmatrix}
\]

which is defined only for multivectors but it can be extended consistently. This makes the first isomorphism in \( (\bigwedge^r \mathbb{F}^{r+s})^* \equiv \bigwedge^r (\mathbb{F}^{r+s})^* \equiv \bigwedge^r \mathbb{F}^{r+s} \) canonical. The second canonical isomorphism comes from the self-duality \( (\mathbb{F}^{r+s})^* \equiv \mathbb{F}^{r+s} \).

**Lemma 24.** Let \( W < \mathbb{F}^{r+s} \) be an arbitrary subspace of rank \( s \) and let \( \mathbf{W}^* \) denote its dual Grassmann coordinate vector. Let \( H < \mathbb{F}^{r+s} \) be an arbitrary subspace of rank \( r \) and let \( \mathbf{H} \) denote its Grassmann coordinate vector. Then \( H \cap W \neq \{0\} \iff \langle \mathbf{W}^*|\mathbf{H}\rangle = 0 \).

**Proof.** Let \( a(1), \ldots, a(s) \) be a basis of \( W \) such that \( \mathbf{W} = a(1) \wedge \cdots \wedge a(s) \). Let \( a(s+1), \ldots, a(s+r) \) be a basis of \( W^\perp \) such that \( \mathbf{W}^* = a(s+1) \wedge \cdots \wedge a(s+r) \). And finally, let \( b(1), \ldots, b(r) \) be a basis of \( H \) such that \( \mathbf{H} = b(1) \wedge \cdots \wedge b(s) \). \( H \cap W \neq \{0\} \) if and only if \( \exists v \in H \) such that \( v \neq 0 \) and \( v \perp W^\perp \). That is,
\( H \cap W \neq \{0\} \) if and only if \( \alpha_1 b(1) + \cdots + \alpha_r b(r) \perp a(s+i) \) for each \( i = 1, \ldots, r \).

This is equivalent with the equation
\[
\begin{vmatrix}
\langle a(s+1)|b(1) \rangle & \cdots & \langle a(s+1)|b(r) \rangle \\
\vdots & \ddots & \vdots \\
\langle a(s+r)|b(1) \rangle & \cdots & \langle a(s+r)|b(r) \rangle 
\end{vmatrix} = 0
\]

Thus, \( H \cap W \neq \{0\} \) if and only if \( \langle W^*|H \rangle = 0 \).

Since the standard basis of the outer power space \( \bigwedge^r \mathbb{F}^{r+s} \) is \( \{e(i_1) \wedge \cdots \wedge e(i_r) \mid 0 \leq i_1 < \cdots < i_r < r+s \} \), where \( \{e(0), \ldots, e(r+s-1)\} \) is the standard basis of \( \mathbb{F}^{r+s} \), the standard scalar product is
\[
\langle L|H \rangle = \sum_{0 \leq i_1 < \cdots < i_r} L_{i_1 \ldots i_r} H_{i_1 \ldots i_r}.
\]

Lemma 25. Let \( \{H(1), \ldots, H(N)\} \) denote the set of the Grassmann coordinate vectors representing the elements of the set \( \mathcal{H} \) of projective \((r-1)\)-subspaces in \( \text{PG}(r+s-1, \mathbb{F}) \). There exists a subspace \( W \) of co-dimension \( r \) (rank \( s \)) in \( \text{PG}(r+s-1, \mathbb{F}) \) meeting each element of \( \mathcal{H} \) if and only if the subspace \( \{H(1)\}^\perp \cap \cdots \cap \{H(N)\}^\perp \leq \text{PG}(r+s-1, \mathbb{F}) \) meets the Grassmann variety \( \mathcal{G}(s,r) \), that is, the linear equation system
\[
\sum_{i_1 < \cdots < i_r} H_{i_1 \ldots i_r}(1)W^*_{i_1 \ldots i_r} = 0, \quad \ldots \quad \sum_{i_1 < \cdots < i_r} H_{i_1 \ldots i_r}(N)W^*_{i_1 \ldots i_r} = 0
\]

together with all the quadratic Plücker relations
\[
\sum_{n=0}^r (-1)^n W^*_{i_1 \ldots i_{r-1} j_n} W^*_{j_0 \ldots j_n \ldots j_r} = 0
\]

(for each 2r-tuple \( (i_1, \ldots, i_{r-1}, j_0, j_1, \ldots, j_r) \) of indices) has nontrivial common solutions for the unknowns \( W^*_{i_1 \ldots i_r} \).

Proof. The quadratic Plücker relations completely determine the Grassmann coordinates of the Grassmannian \( \mathcal{G}(r,s) \subset \text{PG}(r+s-1, \mathbb{F}) \), and thus, they determine the dual Grassmann coordinates of the Grassmannian \( \mathcal{G}(s,r) \).

So, if there exists a dual Grassmann coordinate vector \( W^* \) such that the scalar product \( \langle W^*|H(i) \rangle = 0 \) for each \( i = 1, \ldots, r \) then the orthogonal complementary subspace \( W \) of the subspace \( W^\perp \) coordinatized by \( W^* \) meets
each subspace $H(i)$ coordnatinized by $H(i)$ nontrivially, and thus, $W$ meets each element of $H$ nontrivially.

Conversely, if there exists a subspace $W$ meeting each element of $H$, then its dual Grassmann coordinate vector $W^*$ is orthogonal to each $H(i)$ and its coordinates satisfies the quadratic Plücker relations. □

### 2.2 Lower bound over algebraically closed fields

Since an algebraically closed field contains infinitely many elements, Corollary 6 concludes that the finite set $H$ of $k$-subspaces in $PG(d, \mathbb{F})$ over an algebraically closed field $\mathbb{F}$ could be a set of higgledy-piggledy $k$-subspaces if and only if the condition of Theorem 4 holds.

Chistov et al. [1] stated as a folklore result that no family of cardinality less than $1 + r(n + r)$ can have property $\mathcal{P}_{n,r}(\mathbb{F})$ if the field $\mathbb{F}$ is algebraically closed. For the sake of completeness we give the detailed proof of this folklore result here.

**Lemma 26.** [10, Corollary 3.2.14 and Subsection 3.1.1] The dimension of the Grassmannian as an algebraic variety is $\dim G(r, s) = r \cdot s$ and its degree is

$$\deg G(r, s) = \frac{0!1! \ldots (s-1)!}{r!(r+1)! \ldots (r+s-1)!} (rs)!$$

□

Recall that a projective algebraic variety $G \subset \mathbb{P}$ of dimension $n$ and a projective subspace $S \leq \mathbb{P}$ of co-dimension $n$ always meet over an algebraically closed field.

**Theorem 27.** Over algebraically closed field $\mathbb{F}$, if the set $H$ of $(r - 1)$-subspaces in $PG(r + s - 1, \mathbb{F})$ has at most $r \cdot s$ elements, then there exists a subspace $W$ in $PG(r + s - 1, \mathbb{F})$ of co-dimension $s$ that meets each element of $H$, and thus, $\bigcup H$ is not an $(r - 1)$-generator set.

**Proof.** Suppose that $H = \{H_1, \ldots, H_N\}$ has $N \leq r \cdot s$ elements. If the subspace $H_i$ of rank $r$ is coordnatinized by the homogeneous Grassmann coordinate vector $H(i) \in PG((r+s)^{-1}, \mathbb{F})$, then the Grassmann coordinate vectors of co-$s$-subspaces meeting $H_i$ are the elements of the hyperplane $H(i)^\perp \subset PG((r+s)^{-1}, \mathbb{F})$ orthogonal to the vector $H(i)$.

The subspace $\{H(1)^\perp \cap \cdots \cap H(N)^\perp\}$ has co-dimension at most $N \leq r \cdot s$ in $PG((r+s)^{-1}, \mathbb{F})$ since it is the intersection of $N \leq r \cdot s$ hyperplanes. The
Grassmannian $G(r, s)$ of the $s$-co-dimensional subspaces of $\mathbb{P}G(r + s - 1, \mathbb{F})$ has dimension $r \cdot s$ and its degree $\deg G(r, s)$ is positive.

Thus, $\{H(1)^{}\}^{} \cap \cdots \cap \{H(N)^{}\}^{} \cap G(s, r)$ contains at least $\deg G(r, s) \geq 1$ elements, which are subspaces of co-dimension $r$ meeting all the subspaces in $\mathcal{H}$.

So, using projective parameters $d = r + s - 1$, $k = r - 1$, $r \cdot s = (k+1) \cdot (d-k)$, we have shown that over algebraically closed field $\mathbb{F}$, the set $\mathcal{H}$ of higgledy-piggledy $k$-subspaces in $\mathbb{P}G(d, \mathbb{F})$ has to contain at least $(k + 1) \cdot (d - k) + 1$ elements.

3 Constructions based on the moment curve

Let $\{ (1, t, t^2, \ldots, t^d) : t \in \mathbb{F} \} \cup \{(0, 0, 0, \ldots, 1)\} \subset \mathbb{P}G(d, \mathbb{F})$ be the moment curve (rational normal curve) and let $a(t) = (1, t, t^2, \ldots, t^d)$ denote the coordinate vectors of the points of the moment curve. In this section we investigate collections $\{ H(t) \mid t \in \mathbb{F} \}$ of linear subspaces of rank $r \geq 2$ (projective subspaces of dimension $k = r - 1 \geq 1$) in the vector space $\mathbb{F}^{r+s}$ (in $\mathbb{P}G(d, \mathbb{F})$ where $d = r + s - 1$).

At first, we give a general description for the particular constructions given later in Subsection 3.2, in Subsection 3.3 and in Subsection 3.4.

For each $t \in \mathbb{F}\setminus \{0\}$, the subspace $H(t)$ is coordinatized by the Grassmann coordinate vector $H(t) = a^{[0]}(t) \wedge a^{[1]}(t) \wedge \cdots \wedge a^{[k]}(t)$, where the $i$-th coordinate of the vector $a^{[i]}(t)$ is $a^{[i]}_i(t) = h(i, n) \cdot t^{i-n}$, where $h(i, n) \in \mathbb{F}$ is independent from $t$ and $\forall i : h(i, 0) = 1$, thus $a^{[0]}(t) = a(t)$. The Grassmann coordinates of $H(t)$ are the $r \times r$ subdeterminants of the following matrix.

$$
\begin{bmatrix}
1 & t & t^2 & \cdots & t^{r-1} & t^d \\
h(0,1) \frac{t^1}{1!} & h(1,1) & h(2,1)t & \cdots & h(r-1,1)t^{r-2} & h(d,1)t^{d-1} \\
h(0,2) \frac{t^2}{2!} & h(1,2) \frac{t^2}{2!} & h(2,2) & \cdots & h(r-2,2)t^{r-3} & h(d,2)t^{d-2} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
h(0,k) \frac{t^k}{k!} & h(1,k) \frac{t^k}{k!} & h(2,k) \frac{t^k}{k!} & \cdots & h(k,k) & h(d,k)t^{d-k+1}
\end{bmatrix}
$$

The vectors $a^{[0]}(t), a^{[1]}(t), \ldots, a^{[k]}(t)$ and this matrix above is also well-defined for $t = 0$ if $h(i, n) = 0$ for all $i < n$. If $h(i, n) \neq 0$ for some $i < n$, then the case $t = 0$ shall be handled separately.
Choosing the $i_1$-th, ... $i_r$-th columns, $\frac{t^{i_1} t^{i_2} \cdots t^{i_r}}{t^0 \cdots t^k}$ can be separated, and we get

$$H_{i_1, \ldots, i_r}(t) = \frac{t^{i_1} \cdot t^{i_2} \cdots t^{i_r}}{t^0 \cdots t^k} \cdot \det \begin{bmatrix}
1 & 1 & \cdots & 1 \\
h(i_1, 1) & h(i_2, 1) & \cdots & h(i_r, 1) \\
\vdots & \vdots & \ddots & \vdots \\
h(i_1, k) & h(i_2, k) & \cdots & h(i_r, k)
\end{bmatrix} =$$

$$= t^{i_1 + i_2 + \cdots + i_r} \cdot h(i_1, i_2, \ldots, i_r)$$

using that $0 + 1 + 2 + \cdots + k = \frac{(k+1)k}{2} = \frac{r(r-1)}{2} = \binom{r}{2}$ and using the abbreviation $h(i_1, i_2, \ldots, i_r)$.

Note, that if $H_{i_1, \ldots, i_r}(t) \neq 0$ for at least one $r$-tuple $(i_1, \ldots, i_r)$, then the vectors $a^{[0]}(t), a^{[1]}(t), \ldots, a^{[k]}(t)$ are linearly independent (i.e. the matrix above is of rank $r = k + 1$) and thus, $H(t)$ is well-defined.

**Case when $t$ is zero.** Since $h(i_1, i_2, \ldots, i_r) \cdot t^{i_1 + i_2 + \cdots + i_r - \binom{r}{2}}$ always makes sense for $t = 0$ (even if $h(i, n) \neq 0$ for some $i < n$), define

$$H_{i_1, \ldots, i_r}(0) = h(i_1, i_2, \ldots, i_r) \cdot 0^{i_1 + i_2 + \cdots + i_r - \binom{r}{2}}.$$

We should only see that the multivector coordinatized by the coordinates $H_{i_1, \ldots, i_r}(0) = h(i_1, i_2, \ldots, i_r) \cdot 0^{i_1 + i_2 + \cdots + i_r - \binom{r}{2}}$ is always a totally decomposable multivector (even if the vectors $a^{[0]}(0), \ldots, a^{[k]}(0)$ are not well-defined). One can see that $H_{i_1, \ldots, i_r}(0) = 0$ if $\{i_1, \ldots, i_r\} \neq \{0, 1, \ldots, r - 1\}$, and $H_{0, 1, \ldots, r-1}(0) = h(0, 1, \ldots, r - 1)$. If $h(0, 1, \ldots, r - 1)$ is nonzero then $H(0) = e_0 \land \cdots \land e_{r-1}$, where $e_i$ is the standard basis vector $[0, \ldots, 1, \ldots, 0]$. Thus, we extend the set $\{H(t) \mid t \in \mathbb{F} \setminus \{0\}\}$ by the element coordinatized by the Grassmann coordinate vector $H(0) = e_0 \land \cdots \land e_{r-1}$. (Note that $a^{[0]}(0) \land a^{[1]}(0) \land \cdots \land a^{[k]}(0) = e_0 \land \cdots \land e_{r-1}$ if the vectors $a^{[0]}(0), \ldots, a^{[k]}(0)$ are defined.)

So, we will deal with sets $\{H(t) \mid t \in \mathbb{F}\}$ of subspaces where each subspace $H(t)$ is coordinatized by the Grassmann coordinates $H_{i_1, \ldots, i_r}(t) = h(i_1, \ldots, i_r) \cdot t^{i_1 + \cdots + i_r - \binom{r}{2}}$, where $h(i_1, \ldots, i_r) \in \mathbb{F}$ is independent from $t$. At first, we have a lemma about such sets.

**Lemma 28.** Suppose that $\forall t \in \mathbb{F} : H_{i_1, \ldots, i_r}(t) = h(i_1, \ldots, i_r) \cdot t^{i_1 + \cdots + i_r - \binom{r}{2}}$ are the Grassmann coordinates of the subspace $H(t) \subset \mathbb{F}^{r+s}$ and suppose that
There does not exist any subspace $W < \mathbb{F}^{r+s}$ of co-dimension $r$ (of rank $s$) meeting each $H(t)$ non-trivially if and only if $h(i_1, \ldots, i_r) \neq 0$ for each $r$-tuple $i_1, \ldots, i_r$.

**Proof.** At first, suppose that $h(i_1, \ldots, i_r) \neq 0$ for each $r$-tuple $i_1, \ldots, i_r$ and suppose to the contrary that there exists a subspace $W$ of co-dimension $r$ meeting each subspace $H(t)$. Let $W_{i_1, \ldots, i_r}^*$ $(0 \leq i_1 < \cdots < i_r \leq d)$ denote the dual Grassmann coordinates of $W$. For these Grassmann coordinates we have Plücker relations

$$
\sum_{n=0}^{r} (-1)^n W_{i_1, \ldots, i_r, j_n}^* \cdot W_{j_0, \ldots, j_r}^* = 0
$$

for each $2r$-tuple $i_1, \ldots, i_r, j_0 \ldots j_r$ of indices.

The indirect assumption means that

$$
\sum_{i_1 < \cdots < i_r} W_{i_1, \ldots, i_r}^* \cdot H_{i_1, \ldots, i_r}(t) = \sum_{N=(\binom{r}{2})}^{r \cdot d - (\binom{r}{2})} t^{N-(\binom{r}{2})} \sum_{i_1 < \cdots < i_r} h(i_1, \ldots, i_r) \cdot W_{i_1, \ldots, i_r}^* = 0
$$

for all $t \in \mathbb{F}$. Since the field $\mathbb{F}$ has more than $r \cdot s$ elements, this polynomial above can vanish on each element of $\mathbb{F}$ if only if its each coefficient is zero. So we have $r \cdot s + 1$ new (linear) equations for the dual Grassmann coordinates of $W$:

$$
h(0, 1, \ldots, r-1) \cdot W_{0,1,\ldots,r-1}^* = 0 \quad (N = (\binom{r}{2}))
$$

$$
\vdots
$$

$$
\sum_{i_1 < \cdots < i_r} h(i_1, \ldots, i_r) \cdot W_{i_1, \ldots, i_r}^* = 0 \quad (N)
$$

$$
\vdots
$$

$$
h(d-r+1, \ldots, d) \cdot W_{d-r+1,\ldots,d}^* = 0 \quad (N = rd - (\binom{r}{2}))
$$

Notice that in equation $(N)$ the sum of indices of each dual Grassmann coordinate equals to $N$.  

Suppose by induction that for each \( r \)-tuple \( i_1, \ldots, i_r \) if \( i_1 + \cdots + i_r \leq K \) then \( W_{i_1, \ldots, i_r}^* = 0 \). The first equation then says that \( W_{0,1,\ldots,r-1}^* = 0 \) so the base of induction holds for \( K = \binom{r}{2} \).

Consider the dual Grassmann coordinates \( W_{i_1,\ldots,i_r}^* \) where \( i_1 + \cdots + i_r = K + 1 \). These dual Grassmann coordinates occur in Equation \( (N = K + 1) \):

\[
\sum_{i_1 + \cdots + i_r = K+1 \atop i_1 < \cdots < i_r} h(i_1, \ldots, i_r) \cdot W_{i_1,\ldots,i_r}^* = 0
\]

Lemma 22 says that for each pair \((W_{i_1,\ldots,i_r}^*, W_{j_1,\ldots,j_r}^*)\) of these dual Grassmann coordinates above \((i_1 + \cdots + i_r = K + 1 = j_1 + \cdots + j_r, \{i_1, \ldots, i_r\} \neq \{j_1, \ldots, j_r\}\), there exists a a Plücker relation that has the form

\[
W_{i_1,\ldots,i_r}^* W_{j_1,\ldots,j_r}^* + \Sigma = 0
\]

where \( \Sigma \) is the sum of some products \( W_{k_1,\ldots,k_r} H_{\ell_1,\ldots,\ell_r} \), where \( k_1 + \cdots + k_r < K + 1 < \ell_1 + \cdots + \ell_r \), and thus, using the assumption \( i_1 + \cdots + i_r \leq K \Rightarrow W_{i_1,\ldots,i_r}^* = 0 \), we get

\[
W_{i_1,\ldots,i_r}^* W_{j_1,\ldots,j_r}^* = 0
\]

for each pair \((W_{i_1,\ldots,i_r}^*, W_{j_1,\ldots,j_r}^*)\). These quadratic equations concludes that all \( W_{i_1,\ldots,i_r}^* \) (where \( i_1 + \cdots + i_r = K + 1 \)) should be zero except one. And the linear Equation \((N = K + 1)\) says that this one cannot be exception either.

So we have proved that each dual Grassmann coordinate of the subspace \( W \) of co-dimension \( r \) should be zero, that is a contradiction, since Grassmann coordinates are homogeneous.

**Opposite direction** Suppose that \( h(i_1, \ldots, i_r) = 0 \) for a suitable \( r \)-tuple \( i_1, \ldots, i_r \) and consider the subspace \( W \) of co-dimension \( r \) coordinatized by the following dual Grassmann coordinates. Let \( W_{i_1,\ldots,i_r}^* = 1 \) for the \( r \)-tuple \( i_1, \ldots, i_r \) above, and let \( W_{j_1,\ldots,j_r}^* = 0 \) for the other \( r \)-tuples of indices.

\[
\sum_{j_1 < \cdots < j_r} W_{j_1,\ldots,j_r}^* \cdot H_{j_1,\ldots,j_r}(t) = W_{i_1,\ldots,i_r}^* \cdot H_{i_1,\ldots,i_r}(t) = 1 \cdot 0 \cdot t^{i_1 + \cdots + i_r - \binom{r}{2}} = 0
\]

Thus, \( W \) meets each \( H(t) \) non-trivially. \( \square \)

Note that if the condition of Lemma 28 holds \((h(i_1, \ldots, i_r) \neq 0 \) for each \( r \)-tuple \( i_1, \ldots, i_r \)) then \( H_{0,\ldots,k}(t) = h(0, \ldots, k) \neq 0 \) and thus, the subspace \( H(t) \) is well defined by the Grassmann coordinate vector \( H(t) \).
Corollary 29. Suppose that $|\mathbb{F}| > r \cdot s$. The collection \( \{H(t) \mid t \in \mathbb{F}\} \) of subspaces coordinatized by \( H_{i_1, \ldots, i_r}(t) = h(i_1, \ldots, i_r) \cdot t^{i_1 + \ldots + i_r - \binom{r}{2}} \) is an \( r \)-uniform weak \((s, r \cdot s)\) subspace design if and only if there does not exist a subspace \( W \) of rank \( s \) (co-dimension \( r \)) meeting each \( H(t) \) non-trivially, that is, if and only if \( h(i_1, \ldots, i_r) \neq 0 \) for each \( r \)-tuple \( i_1, \ldots, i_r \).

Proof. If \( \{H(t) \mid t \in \mathbb{F}\} \) is not an \( r \)-uniform weak \((s, r \cdot s)\) subspace design then \( \exists W < \mathbb{F}^{r \cdot s} \) (rank \( W = s \)) such that \( W \) meets more than \( r \cdot s \) elements \( H(t) \) non-trivially. In this case the polynomial \( \sum_{j_1 < \ldots < j_r} W^r_{j_1, \ldots, j_r} \cdot H_{j_1, \ldots, j_r}(t) \) has more than \( r \cdot s \) roots, but its degree is \( r \cdot s \), thus this must be the zero polynomial, and thus, \( w \) meets all the elements \( H(t) \) non-trivially.

If \( \{H(t) \mid t \in \mathbb{F}\} \) is an \( r \)-uniform weak \((s, r \cdot s)\) subspace design then \( \forall W < \mathbb{F}^{r \cdot s} \) of rank \( W = s \) meets at most \( r \cdot s \) elements \( H(t) \), and since \( |\mathbb{F}| > r \cdot s \), \( \exists H(t) \) that meets \( W \) only in the zero vector. \( \square \)

Thus, if \( H_{i_1, \ldots, i_r}(t) = h(i_1, \ldots, i_r) \cdot t^{i_1 + \ldots + i_r - \binom{r}{2}} \) and if we know that \( \{H(t) \mid t \in \mathbb{F}\} \) is a weak \((s, A)\) subspace design with parameter \( r \cdot s < A < |\mathbb{F}| \), then this corollary above prove that \( \{H(t) \mid t \in \mathbb{F}\} \) is an \( r \)-uniform weak \((s, r \cdot s)\) subspace design, moreover, \( h(i_1, \ldots, i_r) \neq 0 \) for each \( r \)-tuple \( i_1, \ldots, i_r \). This will be used to show that known constructions has better (smaller) parameter \( A \) than had been proved.

3.1 Dual constructions

Since we also will investigate constructions of Guruswami and Kopparty \cite{8}, we now give the connection between the techniques used in \cite{8} and the technique shown above.

Consider the collection \( \{H(t) \mid t \in \mathbb{F}\} \) of subspaces coordinatized by the Grassmann coordinate vectors \( \mathbf{H}(t) = a[0](t) \wedge a[1](t) \wedge \cdots \wedge a[k](t) \). Then the orthogonal complementary subspace of \( H(t) \) is the intersection of hyperplanes: \( H(t)^\perp = \{a[0](t)^\perp \cap \{a[1](t)^\perp \cap \cdots \cap \{a[k](t)^\perp \} \} \).

The co-vector \( \mathbf{b} = [b_0, \ldots, b_d] \in (\mathbb{F}^{d+1})^* \) is perpendicular to the coordinate vector \( a[n](t) \in \mathbb{F}^{d+1} \) if and only if \( \sum_{j=1}^d b_j \cdot h(j, n) \cdot t^{i_j - n} = 0 \). This motivates the following notations.

Notation. For the coordinate vector \( z = [z_0, z_1, \ldots, z_d] \in \mathbb{F}^{d+1} \) let \( P_z(X) = \sum_{j=0}^d z_j X^j \in \mathbb{F}[X] \) denote a univariate polynomial of degree at most \( d \), and let \( P_z[n](X) = \sum_{j=i}^d z_j \cdot h(n, j) \cdot X^{j-n} \in \mathbb{F}[X] \). Note that \( P_z[0](X) = P_z(X) \).
Remark 30. Note that $P_{2}^{[n]}(X)$ is a rational function, moreover, it is the quotient of a polynomial of degree $d$ with $X^n$. The function $P_{2}^{[n]}(X)$ is a polynomial (of degree $d - n$) if and only if $\forall i < n : h(i, n) = 0$.

The co-vector $b = [b_0, \ldots, b_d] \in (\mathbb{F}^{d+1})^*$ is perpendicular to the homogeneous coordinate vector $a^{[n]}(t) \in \mathbb{F}^{d+1}$ if and only if $P_{b}^{[n]}(t) = 0$, thus the annihilator subspace $H(t)^\perp = a^{[0]}(t)^\perp \cap a^{[1]}(t)^\perp \cap \cdots \cap a^{[k]}(t)^\perp$ equals to the subspace $\{b \in (\mathbb{F}^{d+1})^* \mid P_{b}^{[n]}(t) = 0 : \forall n = 0, 1, \ldots, k\}$ equals to $(\mathbb{F}^{d+1})^*$.

Let the arbitrary linear subspace $W \leq \mathbb{F}^{d+1}$ of rank $s$ be fixed and consider the set of polynomials $\{P_{b}(X) \mid b \in W^\perp\} \subset \mathbb{F}[X]$. This subset is a linear subspace of $\mathbb{F}[X]$ and it is isomorphic to $W^\perp$ via the linear map $b \mapsto P_{b}(X)$. The constructions of Guruswami and Kopparty [8] are based on this isomorphism.

Let $\{b(1), \ldots, b(r)\} \subset (\mathbb{F}^{d+1})^*$ be a basis of $W^\perp$ and, using Gaussian elimination, without loss of generality we can suppose that the last $j - 1$ coordinates of $b(j)$ are zero, that is, $\deg P_{b(j)}(X) \leq d - j + 1$.

The following matrix

$$M(X) = \begin{bmatrix}
P_{b(1)}(X) & P_{b(2)}(X) & \cdots & P_{b(r)}(X) \\
P_{b(1)}[1](X) & P_{b(2)}[1](X) & \cdots & P_{b(r)}[1](X) \\
\vdots & \vdots & \ddots & \vdots \\
P_{b(1)}[k](X) & P_{b(2)}[k](X) & \cdots & P_{b(r)}[k](X)
\end{bmatrix}$$

is a square matrix since $r = k + 1$. The linear map $b \mapsto P_{b}(t)$ maps the subspace $H(t)^\perp \cap W^\perp$ to the kernel of $M(t)$. If $h(i, n) = 0 : \forall i < n$ then this matrix is a polynomial matrix (each element is a univariate polynomial), thus, its determinant is also a polynomial. For completeness, we prove here the following easy statement.

Lemma 31. Let $M(X) \in \mathbb{F}[X]^{n \times m}$ be an $m \times m$ matrix of polynomials. For each element $t \in \mathbb{F}$, if $\det M(t) = 0$ then $t$ is the root of the polynomial $\det M(x)$ of multiplicity at least $R = \text{rank ker}(M(t))$.

Proof. Let $t \in \mathbb{F}$ be an arbitrary element of the field and consider the matrix $M(t) \in \mathbb{F}^{n \times m}$ and its kernel $\text{ker}(M(t)) \leq \mathbb{F}^m$ of rank $R = \text{rank ker}(M(t))$. Let $a^{(i)}, \ldots, a^{(R)}, a^{(R+1)}, \ldots, a^{(m)}$ be such a basis of $\mathbb{F}^m$ that $a^{(i)}, \ldots, a^{(R)}$ is
the basis of \( \ker(M(t)) \) and \( \det A = 1 \) where \( A = [a^{(1)}, \ldots, a^{(m)}] \).

\[
M(t)A = \begin{bmatrix}
0 & \ldots & 0 & * & \ldots & * \\
0 & \ldots & 0 & * & \ldots & * \\
\vdots & & \vdots & & \vdots & \\
0 & \ldots & 0 & * & \ldots & *
\end{bmatrix}
\]

Thus, the elements of the first \( R \) columns of the matrix \( M(X)A \) are polynomials vanishing on \( X = t \), thus the linear polynomial \( (X - t) \) divides them. So \( \det(M(X)) = \det(M(X)A) = (X - t)^R \cdot f(X) \) where \( f(X) \in \mathbb{F}[X] \).

**Lemma 32.** Suppose that \( h(i_1, \ldots, i_r) \neq 0 \) for all \( \{i_1, \ldots, i_r\} \) and suppose that \( h(i, n) = 0 : \forall i < n \). Then the collection \( \{H(t) \mid t \in \mathbb{F}\} \) of subspaces perpendicular to the subspaces coordinatized by the Grassmann coordinates \( H_{i_1, \ldots, i_r}(t) = h(i_1, \ldots, i_r) \cdot t^{i_1 + \cdots + i_r} \binom{2}{r} \) is an \( s \)-uniform strong \((r, s \cdot r)\) subspace design.

Moreover, in this case, the collection \( \{H(t) \mid t \in \mathbb{F}\} \) of subspaces coordinatized by the Grassmann coordinates \( H_{i_1, \ldots, i_r}(t) = h(i_1, \ldots, i_r) \cdot t^{i_1 + \cdots + i_r} \binom{2}{r} \) is an \( r \)-uniform strong \((s, r \cdot s)\) subspace design.

**Proof.** Using Lemma 31 above we can see that

\[
\sum_{t \in \mathbb{F}} \text{rank}(H(t) \perp \cap W^\perp) \leq \sum_{t \in \mathbb{F}} \text{mult}(\det(M(X), t) \leq \deg \det M(X)
\]

if \( \det M(X) \neq 0 \) (if it is not the zero polynomial).

Since \( h(i_1, \ldots, i_r) \neq 0 \) for all \( \{i_1, \ldots, i_r\} \), thus, Corollary 29 says that \( \{H(t) \mid t \in \mathbb{F}\} \) is a \( r \)-uniform weak \((s, r \cdot s)\) subspace design. Theorem 9 says that in this case \( \{H(t) \perp \mid t \in \mathbb{F}\} \) is an \( s \)-uniform weak \((r, s \cdot r)\) subspace design. So, for each subspace \( W \) of rank \( s \), the subspace \( W^\perp \) of rank \( r \) does not block all the subspaces \( H(t) \perp \), thus, the polynomial \( \det M(X) \) cannot be zero for all substitution \( X = t \).

Remember that \( \deg P_{b(j)} \leq d - j + 1 \), and we know that for arbitrary polynomial \( P(X) \) the degree \( \deg P_{b(j)}(X) = \deg P(X) - i \). Since \( \det M(X) = \sum_{\sigma \in S_r} (-1)^{i(\sigma)} \prod_{j=1}^s P_{b(j)}^{i-1}(x), \text{deg} \det M(X) \leq \sum_{j=1}^s (d - \sigma j + 1 - (j - 1)) = s \cdot d - \sum_{j=1}^s (\sigma j) - \sum_{j=1}^s j = s \cdot d - 2 \binom{s}{2} = s \cdot (d - s + 1).

Thus,

\[
\sum_{t \in \mathbb{F}} \text{rank}(H(t) \perp \cap W^\perp) \leq \deg \det M(X) \leq s \cdot (d - s + 1)
\]
So the collection \( \{ H(t)^\perp : t \in \mathbb{F}\} \) of subspaces in \((\mathbb{F}^{s+r})^*\) is an \( s \)-uniform \((r, s \cdot r)\) strong subspace design, where \( r = d - s + 1 \).

The last statement comes directly from Theorem 15. \( \square \)

Finally, we consider the particular constructions, at first the most basic construction, the tangents of the moment curve.

### 3.2 Tangents of the moment curve

In this subsection we suppose that the the characteristic of the field \( \mathbb{F} \) is bigger than \( r + s \), since the derivatives could vanish otherwise, making errors in the proofs.

Let \( h(i, n) = \frac{d}{(i-n)^2} \) if \( i \geq n \), and let \( h(i, n) = 0 \) if \( i < n \). Then \( a^{[n]}(t) \) is the \( n \)-th derivate of \( a(t) \) as a \((d+1)\)-tuple of polynomials of variable \( t \). The subspace \( H(t) \) coordinatized by the Grassmann coordinate vector \( H(t) = a^{[0]}(t) \land a^{[1]}(t) \land \cdots \land a^{[k]}(t) \) is the ‘tangent subspace of rank \( r \)’ of the moment curve.

The dual construction \( \{ H(t)^\perp : t \in \mathbb{F} \} \) is exactly the basic construction of Guruswami and Kopparty [8, Subsection 5.1] based on multiplicity codes. Thus, Theorem 13 says that \( \{ H(t)^\perp : t \in \mathbb{F} \} \) is an \( s \)-uniform strong \((r, r \cdot s)\) subspace design.

Thus, according to Theorem 15, \( \{ H(t) : t \in \mathbb{F} \} \) is an \( r \)-uniform strong \((s, r \cdot s)\) subspace design. And thus, it is also an \( r \)-uniform weak \((s, r \cdot s)\) subspace design. So, we have seen that \( h(i_1, \ldots, i_r) \neq 0 \) for each \( r \)-tuple \( i_1, \ldots, i_r \) if the characteristic of the field \( \mathbb{F} \) is big enough. The following constructions are made to eliminate the problem of small characteristics, so, from now on, the characteristic of the field \( \mathbb{F} \) is again arbitrary.

### 3.3 Diverted tangents of the moment curve

In our previous article [3], we solve the problem of small characteristics by ‘diverting’ the tangent lines of the moment curve. The ‘almost generalization’ of this idea is the following. (Almost, because the case \( r = 2 \) is not exactly the same that the ‘diverted tangent lines’ in that article, but the technique is very similar.)

Let \( \omega \in \mathbb{F} \setminus \{0\} \) be a suitable element and let \( h(i, n) = (\omega^i)^{i-r} \) if \( i \geq r \) or if \( i = n < r \), and let \( h(i, n) = 0 \) otherwise. So, the elements \( h(i_1, \ldots, i_r) \) are
the $r \times r$ subdeterminants of the following $r \times d$ matrix.

\[
\begin{bmatrix}
1 & 0 & 0 & \ldots & 0 & 0 & 1 & 1 & \ldots & 1 \\
0 & \omega^{1-r} & 0 & \ldots & 0 & 0 & 1 & \omega^1 & \ldots & \omega^{d-r} \\
0 & 0 & \omega^{2(2-r)} & \ldots & 0 & 0 & 1 & \omega^2 & \ldots & \omega^{2(d-r)} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \ldots & \omega^{(r-2)(-2)} & 0 & 1 & \omega^{r-2} & \ldots & \omega^{(r-2)(d-r)} \\
0 & 0 & 0 & \ldots & 0 & \omega^{(r-1)(-1)} & 1 & \omega^{r-1} & \ldots & \omega^{(r-1)(d-r)}
\end{bmatrix}
\]

Consider the $r$-tuple of indices $0 \leq i_1 < \cdots < i_r \leq d$ where $i_R \leq r - 1 < r \leq i_{R+1}$ and let $0 \leq j_1 < \cdots < j_{r-R} \leq r - 1$ denote the integers such that \( \{i_1, \ldots, i_R, j_1, \ldots, j_{r-R}\} = \{0, 1, \ldots, r - 1\} \). Using these notations one can easily see that

\[
h(i_1, \ldots, i_r) = \pm \omega^{i_1(i_1-r) + \cdots + i_R(i_R-r)} \cdot \det \Omega \quad \text{where} \quad \Omega_{kl} = \omega^{j_k(i_1-r+k)}.
\]

In particular, \( h(0,1,\ldots,r-1) = \omega^{q(1-r)+(4-2r)+\cdots+(1-r)} \neq 0 \). If \( i_1 \geq r \) then \( h(i_1, \ldots, i_r) = V(\omega^{i_1-r}, \ldots, \omega^{i_r-r}) \) and if \( i_1 = r - 1 \) then \( h(i_1, \ldots, i_r) = \pm \omega^{1-r} \cdot V(\omega^{2-r}, \ldots, \omega^{j_r-r}) \), where \( V(a_1, \ldots, a_N) \) denotes the Vandermonde determinant, which is nonzero if and only if the elements \( a_1, \ldots, a_N \) are distinct. So \( \omega \) has to be an element of order more than \( d - r = s - 1 \).

There is a little problem with the numbers \( h(i_1, \ldots, i_r) \) if some of the indices are less than \( r - 1 \) and some of them are bigger. The determinant of \( \Omega \) is a \textit{generalized Vandermonde determinant}.

**Definition 33.** Let \( 0 \leq j_1 < j_2 < \cdots < j_N \) be a strictly increasing series of non-negative integers and let \( a_1, \ldots, a_N \) be elements of the field \( \mathbb{F} \). The \textit{generalized Vandermonde} matrix and determinant is defined as the matrix \( V \) of entries \( V_{k\ell} = a_k^{j_\ell} \) and its determinant, respectively. If \( j_i = i - 1 \) then they are the well known Vandermonde matrix and determinant.

We have a very special case of \textit{generalized Vandermonde} matrices here, where \( a_k = \omega^{-r+i_{R+k}} \).

**Remark 34.** The generalized Vandermonde determinant is totally positive over \( \mathbb{R} \) if \( a_1 < \cdots < a_r \) are distinct positive elements of \( \mathbb{R} \). So, if \( Q \subset F \) (that is, if \( \text{char } F = 0 \)) then \( \omega \in Q, \omega > 1 \) is a suitable element. But, if \( \text{char } F = p \neq 0 \) then a generalized Vandermonde determinant of distinct elements can be zero.
Since the generalized Vandermonde determinant is an alternating multivariate polynomial of the variables \( a_1, \ldots, a_N \), it is the product of the Vandermonde determinant \( V(a_1, \ldots, a_N) \) and a symmetric polynomial of these variables.

Let \( N \) denote \( r - R \) and let \( b_k = i_{R+k} - r \). Our generalized Vandermonde determinant

\[
\det \Omega = \sum_{\sigma \in S_N} (-1)^{l(\sigma)} \prod_{k=1}^{N} \omega^{(-r+i_{R+k})} j_{\sigma k} = \sum_{\sigma \in S_N} (-1)^{l(\sigma)} \sum_{k=1}^{N} b_k \cdot j_{\sigma k}
\]

which is a univariate polynomial of \( \omega \) and the polynomial \( \det \Omega \) is divisible by the Vandermonde determinant

\[
V(\omega^{b_1}, \ldots, \omega^{b_N}) = \prod_{1 < j} (\omega^{b_j} - \omega^{b_i})
\]

which is also a univariate polynomial of \( \omega \). The following lemma gives degrees of these polynomials.

**Lemma 35.** Let \( 0 \leq j_1 < j_2 < \cdots < j_N \leq r - 1 \) an let \( 0 \leq b_1 < b_2 < \cdots < b_N \leq d - r \) be integers and for each permutation \( \sigma \in S_N \) let \( \Sigma(\sigma) \) denote the sum

\[
\Sigma(\sigma) = \sum_{k=1}^{N} b_k \cdot j_{\sigma k}
\]

Using these notations, for each non-identical permutation \( \sigma \neq \text{id} : \Sigma(\sigma) < \Sigma(\text{id}) \leq N \cdot (d - r) \cdot (r - 1) - \left( \begin{array}{c} N \\end{array} \right) \cdot \frac{d}{2} \). Moreover, \( \max \Sigma(\sigma) - \min \Sigma(\sigma) \leq \frac{N(d-r)(r-1)}{2} \).

**Proof.** The strict inequality \( \Sigma(\sigma) < \Sigma(\text{id}) \) comes by induction from the following fact. Suppose that \( \sigma k > \sigma(k + 1) \). (Such a \( k \) exists if and only if \( \sigma \neq \text{id} \)). Then let \( \sigma' \ell = \sigma \ell \) for each \( \ell \neq k, \ell \neq (k + 1) \), and let \( \sigma' k = \sigma(k + 1) < \sigma k = \sigma'(k + 1) \). Then \( \Sigma(\sigma') - \Sigma(\sigma) = b_k \cdot j_{\sigma(k+1)} + b_{k+1} \cdot j_{\sigma k} - b_k \cdot j_{\sigma k} - b_{k+1} \cdot j_{\sigma(k+1)} = (b_{k+1} - b_k) \cdot (j_{\sigma k} - j_{\sigma(k+1)}) > 0 \cdot 0 \). By induction in the number of inversions we get the result. The same induction shows that \( \min \Sigma(\sigma) = \Sigma(\text{opp}) = \sum_{k=1}^{N} b_k \cdot j_{N+1-k} \) where opp \( \in S_N \) denotes the opposite permutation.
First bound  $\Sigma(id) = \sum_{k=1}^{N} b_k \cdot j_k \leq \sum_{k=0}^{N-1} (d-r-k)(r-1-k) = \sum_{k=0}^{N-1} ((d-r)(r-1) - k(d-1) + k^2) = N(d-r)(r-1) - \binom{N}{2}(d-1) + \frac{6}{(N-1)N(2N-1)} = N(d-r)(r-1) + \binom{N}{2} \left( \frac{2N-1}{3} - d + 1 \right) = N(d-r)(r-1) - \binom{N}{2} \frac{3d-2(N+1)}{3}$. Since $N+1 \leq d$, the first bound comes.

Second bound  $2(\Sigma(id) - \Sigma(opp)) = \sum_{k=1}^{N} j_k \cdot (b_k - b_{N+1-k}) + \sum_{k=1}^{N} j_{N+1-k} \cdot (b_{N+1-k} - b_k) = \sum_{k=1}^{N} (j_k - j_{N+1-k})(b_k - b_{N+1-k}) \leq \sum_{k=1}^{N} (r-1)(d-r) = N(r-1)(d-r)$.

Corollary 36. Since $\Sigma(\sigma) < \Sigma(id)$ if $\sigma \neq id$, the leading term of the univariate polynomial $\det \Omega$ is $\omega^{\Sigma(id)}$, thus, this polynomial is not the zero polynomial and its degree is $\max \Sigma(\sigma) \leq N \cdot (d-r) \cdot (r-1) - \binom{N}{2} \cdot \frac{d}{3}$, moreover, $\det \Omega$ is the product of $\omega^{\Sigma(opp)}$ and a polynomial of degree at most $\max \Sigma(\sigma) - \min \Sigma(\sigma) \leq N(d-r)(r-1) - \binom{N}{2}(d-r)$.

Since $N \leq r$, the polynomial $\det \Omega$ has at most $\binom{N}{2}(d-r)$ nonzero roots. Moreover, since the coefficients of $\det \Omega$ are the sums of $\pm 1$, each root is in the extension field of the prime field $F_p$ of degree at most $\binom{N}{2}(d-r)$, so their order is at most $p^{\binom{N}{2}(d-r) - 1}$.

Thus, the requirements $h(i_1, \ldots, i_r) \neq 0$ are polynomial conditions for the element $\omega$. If $\omega$ is not a soluiton of any of the polynomials $\omega^{j(i_1-r)+\cdots+i_r(i_r-r)}$, $\det \Omega(\omega)$, then $h(i_1, \ldots, i_r) \neq 0$ for each $r$-tuple $i_1, \ldots, i_r$.

Theorem 37. Let $r$ and $s$ be given and suppose that $\text{char } F = p \neq 0$. If $F$ has more than $\binom{r+s}{r} (s-1)$ elements, or if the field has $q = p^h$ elements and $h > \binom{N}{2}(s-1)$, then there exists an $r$-uniform strong $(s, r \cdot s)$ subspace design, and an $s$-uniform strong $(r, s \cdot r)$ subspace design in the vector space $F^{r+s}$.

Proof. Let $d = r+s-1$ and suppose that $F$ has more than $p^{\binom{N}{2}(d-r)}$ elements. If $F = F_q$, where $q = p^h$, $h > \binom{N}{2}(d-r)$, then the order of a primitive element $\omega \in F_q$ is $p^h - 1 > p^{\binom{N}{2}(d-r)} - 1$. If $F$ is infinite then it has element $\omega$ of order more than $p^{\binom{N}{2}(d-r)} - 1$. Corollary 36 above yields that if the order of $\omega$ is bigger than $p^{\binom{N}{2}(d-r)} - 1$, then $\omega$ cannot be the solution of any of the equations $h(i_1, \ldots, i_r) = 0$.

Suppose that $F$ has more than $p^{\binom{N}{2}(d-r)}$ elements. Then the number of distinct roots of all the polynomials $\det \Omega$ (for all $r$-tuples) is smaller...
than $|\mathbb{F}|$ so $\exists \omega \in \mathbb{F}$ such that $\omega$ is not the solution of any of the equations $h(i_1, \ldots, i_r) = 0$.

If we choose the element $\omega$ properly, Lemma 32 says that the set of diverted tangents of the moment curve is an $r$-uniform strong $(s, r \cdot s)$ subspace design, and the orthogonal complementary subspaces of the diverted tangents constitutes an $s$-uniform strong $(r, s \cdot r)$ subspace design.

If the characteristic $p$ of the field $\mathbb{F}_q$ is smaller than $r + s$ and $q < {r+s \choose r} (s - 1)$ and $q = p^h$ and $h \leq {\lfloor \frac{r}{2} \rfloor} (s - 1)$ then the theorem above does not work. In this case we have to use another construction yielding strong subspace designs of parameter $A$ bigger than $r \cdot s$, but we will see that this parameter $A$ is $r \cdot s$ if we consider the subspace design as a weak subspace design.

### 3.4 Secants of the moment curve

Consider the diverted tangents of the moment curve. Since $V(\omega^{i_1}, \ldots, \omega^{i_r}) \cdot t^{i_1 + \cdots + i_r - \lfloor \frac{r}{2} \rfloor}$ is not meaningless if some index $i_k < r$, we can extend the definition of $H_{i_1, \ldots, i_r}(t) = V(\omega^{i_1}, \ldots, \omega^{i_r}) \cdot t^{i_1 + \cdots + i_r - \lfloor \frac{r}{2} \rfloor}$ to the all $r$-tuples of indices. In this case $h(i, n) = (\omega^n)^i$ for all $i$ and $n$.

Since for $t \neq 0 H(t)$ is the subspace containing the points of the moment curve $a(t), a(\omega t), a(\omega^2 t), \ldots, a(\omega^{r-1} t)$ (remember that the vector $\frac{1}{t} a(\omega^n t)$ and the vector $a(\omega^n t)$ coordinatize the same projective point if $t \neq 0$) these subspaces will be called the $\omega$-secants of the moment curve.

Since $i_r \leq d = r + s - 1$, $V(\omega^{i_1}, \ldots, \omega^{i_r}) \neq 0$ if (and only if) the order of $\omega$ is at least $r + s$. Suppose that $|\mathbb{F}| > r + s$ and let $\omega \in \mathbb{F}$ such a suitable element. Corollary 29 of Lemma 28 says that the set $\{H(t) \mid t \in \mathbb{F}\}$ of the $\omega$-secants of the moment curve is an $r$-uniform weak $(s, r \cdot s)$ subspace design.

Consider the orthogonal complementary subspaces of the $\omega$-secants. It is exactly the basic construction of Guruswami and Kopparty [8, Subsection 4.1] based on Reed-Solomon codes and Theorem 13 says that $\{H(t) \mid t \in \mathbb{F}\}$ is an $s$-uniform strong $(r, s \cdot r + \lfloor \frac{r}{2} \rfloor)$ subspace design. Thus, according to Theorem 15, the set $\{H(t) \mid t \in \mathbb{F}\}$ of the $\omega$-secants of the moment curve is an $r$-uniform strong $(s, r \cdot s + \lfloor \frac{r}{2} \rfloor)$ subspace design.

According to Theorem 9, Guruswami–Kopparty construction $\{H(t) \mid t \in \mathbb{F}\}$ based on Reed-Solomon codes is an $s$-uniform weak $(r, r \cdot s)$ subspace design.
4 Concluding remarks

Let the natural numbers \( r \geq 2 \) and \( s \geq 2 \) be given and let \( \mathbb{F} \) be an arbitrary field of more than \( r + s \) elements. Then the constructions above prove that there exist \( r \)-uniform strong \((s, r \cdot s + \min\{ \binom{r}{2}, \binom{s}{2} \})\) subspace designs in \( \mathbb{F}^{r+s} \).

Moreover, there exist \( r \)-uniform strong \((s, r \cdot s)\) subspace designs in \( \mathbb{F}^{r+s} \):

- if \( \text{char} \mathbb{F} = 0 \), or
- if \( \text{char} \mathbb{F} = p > r + s \), or
- if \( |\mathbb{F}| > \binom{r+s}{r} \binom{s}{2} (s - 1) \), or
- if \( |\mathbb{F}| > p^{\binom{r}{2} (s-1)} \) where \( p = \text{char} \mathbb{F} \).

The constructions also prove that there exist \( r \)-uniform weak \((s, r \cdot s)\) subspace designs in \( \mathbb{F}^{r+s} \), thus, for arbitrary \( k \geq 1 \) and \( d \geq 3 \) there exist \((k+1) \cdot (d-k) + 1\) projective \( k \)-subspaces of \( \text{PG}(d, \mathbb{F}) \) in higgledy-piggledy arrangement.

4.1 Some open questions

The construction of \((k+1) \cdot (d-k) + 1\) projective \( k \)-subspaces of \( \text{PG}(d, \mathbb{F}) \) in higgledy-piggledy arrangement is the smallest one over algebraically closed field \( \mathbb{F} \). Over other fields we have a much smaller lower bound, but we do not know whether there are smaller sets of higgledy-piggledy \( k \)-subspaces or not. We do not know the tight lower bound over non-closed fields.

We prove that the diverted tangents of the moment curve is a good construction if the field has more than \( \binom{r+s}{r} \binom{s}{2} (s - 1) \) elements or more than \( p^{\binom{r}{2} (s-1)} \) elements where \( p = \text{char} \mathbb{F} \), but we do not know whether this construction works well also over some smaller fields. We conjecture that it does.

4.2 Recent improvements by Forbes and Guruswami

After we had submitted this article, Forbes and Guruswami [7] have further improved some results about subspace designs. A new result [7, Theorem 2.8] sharpened further the first bound of our old theorem cited here as Theorem 13, proving that \( A \leq \frac{(m-s)^s}{m-r-(s-1)} \) for also the first Guruswami–Kopparty construction (in the case \( h = 1 \)).
Remark 38. Using the further sharpened bounds of [7, Theorem 2.8], we get that for given $s \geq 2$ and $r \geq 2$, both Guruswami–Kopparty constructions give us $r$-uniform strong $(s, r \cdot s)$ subspace designs if the field $\mathbb{F}$ has more than $r + s$ elements.

Another achievement of Forbes and Guruswami is [7, Proposition 6.1] proving that subspace designs and lossless seeded rank condensers are the same object. Forbes and Shpilka [4] had already constructed rank condensers using error-correcting codes (and together with Saptharishi [5] they improved their results); see also [6]. The method of [4] seems to be equivalent to our constructions in a different 'language'.

4.3 Final remarks

We are grateful to the anonymous referees for their useful comments including reminding us of the recent work [7] and some prior works.

One of the referees gave an alternative proof of Theorem 9, using matrices and transposes as follows. Consider an $r \times n$ matrix $A$ and an $n \times r$ matrix $B$. We can think of $A$ as a linear map $\mathbb{F}^n \to \mathbb{F}^r$ and $B$ as a dimension $r$ subspace of $\mathbb{F}^n$. Then kernel of the map $A$ is then $A^\perp$, and thus the rank of $AB$ is $A^\perp \cap B$. The main point is that $\text{rank}(AB) = \text{rank}(B^\top A^\top)$, where $\top$ is the transpose. In the context of subspace designs, one can take a subspace $H_i$ in the design, and let $B$ be a matrix with columns space equalling $H_i$, and let $A$ be a matrix with row-span $W^\perp$. Then we see that $\text{rank}(AB) = \dim(H_i \cap W)$. By using the transpose, we see that $\dim H^\perp - \dim(W^\perp \cap H^\perp) = \dim W - \dim(H \cap W)$. In this setting of parameters, $\dim H^\perp = \dim W$, and thus $\dim(W^\perp \cap H^\perp) = \dim(H \cap W)$. This thus clearly shows that duals of subspace designs with these parameters are still subspace designs with comparable parameters.

References


[10] Laurent Manivel (Author); John R. Swallow (Translator): *Symmetric functions, Schubert polynomials and degeneracy loci*. SMF/AMS Texts