



The Plücker embedding in algebraic cryptanalysis

Lars Ran

August 11, AM-PQC, Ohrid

As cryptanalysts we are sometimes interested in finding secret subspaces

As cryptanalysts we are sometimes interested in finding secret subspaces

For example:

As cryptanalysts we are sometimes interested in finding secret subspaces

For example:

- ▷ the oil space in UOV

As cryptanalysts we are sometimes interested in finding secret subspaces

For example:

- ▷ the oil space in UOV
- ▷ the rowspace or kernel space of the secret matrix in MinRank

As cryptanalysts we are sometimes interested in finding secret subspaces

For example:

- ▷ the oil space in UOV
- ▷ the rowspace or kernel space of the secret matrix in MinRank
- ▷ the image in the subcode equivalence problem

Usually, a k -dimensional secret subspace V of $\mathbb{F}_q^n$ is modeled as

$$G = \begin{bmatrix} 1 & 0 & \cdots & 0 & x_{11} & x_{12} & \cdots & x_{1(n-k-1)} & x_{1(n-k)} \\ 0 & 1 & \cdots & 0 & x_{21} & x_{22} & \cdots & x_{2(n-k-1)} & x_{2(n-k)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & x_{k1} & x_{k2} & \cdots & x_{k(n-k-1)} & x_{k(n-k)} \end{bmatrix}$$

Usually, a k -dimensional secret subspace V of $\mathbb{F}_q^n$ is modeled as

$$G = \begin{bmatrix} 1 & 0 & \cdots & 0 & x_{11} & x_{12} & \cdots & x_{1(n-k-1)} & x_{1(n-k)} \\ 0 & 1 & \cdots & 0 & x_{21} & x_{22} & \cdots & x_{2(n-k-1)} & x_{2(n-k)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & x_{k1} & x_{k2} & \cdots & x_{k(n-k-1)} & x_{k(n-k)} \end{bmatrix}$$

This representation is unique but does not always exist

	Kipnis–Shamir	Plücker
representative of V	$G = [I_k G']$	
ambient space	$\mathbb{F}^{k \times (n-k)}$	

$$V^\perp$$

$$\mathbf{x} \overset{?}{\in} V$$

$$\mathbf{x} \overset{?}{\perp} V$$

$$\mathbf{x} \in V$$

$$W \subset V$$

Building the dictionary

$$[n] = \{1, \dots, n\}$$

$\mathbf{e}_1, \dots, \mathbf{e}_n$ will be the standard basis of $\mathbb{F}_q^n$

$\text{Gr}(k, n)$ is the set of all k dimensional subspaces of $\mathbb{F}_q^n$

$G_{*,J}$ is the submatrix of G with columns indexed by J

I, J , and K are indexing subsets of $[n]$

Encoding the maximal minors

Consider the vector space $\bigwedge^k \mathbb{F}^n \cong \mathbb{F}^{\binom{n}{k}}$ labeled by the k -subsets of $[n]$

$$\bigwedge^k \mathbb{F}^n = \langle \mathbf{e}_I : I \subset [n], |I| = k \rangle$$

Encoding the maximal minors

Consider the vector space $\bigwedge^k \mathbb{F}^n \cong \mathbb{F}^{\binom{n}{k}}$ labeled by the k -subsets of $[n]$

$$\bigwedge^k \mathbb{F}^n = \langle \mathbf{e}_I : I \subset [n], |I| = k \rangle$$

We can send any $k \times n$ matrix G to an element of $\bigwedge^k \mathbb{F}^n$ by taking maximal minors indexed by columns

$$G \mapsto \sum_{|I|=k} \det(G_{*,I}) \cdot \mathbf{e}_I$$

Encoding the maximal minors

Consider the vector space $\bigwedge^k \mathbb{F}^n \cong \mathbb{F}^{\binom{n}{k}}$ labeled by the k -subsets of $[n]$

$$\bigwedge^k \mathbb{F}^n = \langle \mathbf{e}_I : I \subset [n], |I| = k \rangle$$

We can send any $k \times n$ matrix G to an element of $\bigwedge^k \mathbb{F}^n$ by taking maximal minors indexed by columns

$$\iota : \mathbb{F}^{k \times n} \rightarrow \mathbb{F}^{\binom{n}{k}}$$

$$G \mapsto \sum_{|I|=k} \det(G_{*,I}) \cdot \mathbf{e}_I$$

The Plücker embedding

All generator matrices of U can be written as SG for some $S \in GL_k$. If we want to use ι to model a subspace, it should be invariant on this choice

The Plücker embedding

All generator matrices of U can be written as SG for some $S \in \mathrm{GL}_k$. If we want to use ι to model a subspace, it should be invariant on this choice

Let's see

$$\det((SG)_{*,I}) = \det(S(G_{*,I})) = \det(S) \det(G_{*,I})$$

The Plücker embedding

All generator matrices of U can be written as SG for some $S \in \mathrm{GL}_k$. If we want to use ι to model a subspace, it should be invariant on this choice

Let's see

$$\det((SG)_{*,I}) = \det(S(G_{*,I})) = \det(S) \det(G_{*,I})$$

And thus

$$\iota(SG) = \sum_{|I|=k} \det((SG)_{*,I}) \cdot \mathbf{e}_I = \sum_{|I|=k} \det(S) \det(G_{*,I}) \cdot \mathbf{e}_I = \det(S) \cdot \iota(G)$$

The Plücker embedding

All generator matrices of U can be written as SG for some $S \in \mathrm{GL}_k$. If we want to use ι to model a subspace, it should be invariant on this choice

Let's see

$$\det((SG)_{*,I}) = \det(S(G_{*,I})) = \det(S) \det(G_{*,I})$$

And thus

$$\iota(SG) = \sum_{|I|=k} \det((SG)_{*,I}) \cdot \mathbf{e}_I = \sum_{|I|=k} \det(S) \det(G_{*,I}) \cdot \mathbf{e}_I = \det(S) \cdot \iota(G)$$

Therefore this descends to a map

$$\hat{\iota} : \mathrm{Gr}(k, n) \rightarrow \mathbb{P}(\bigwedge^k \mathbb{F}^n)$$

which is the Plücker embedding

	Kipnis–Shamir	Plücker
V	$G = [I_k G']$	$\mathcal{G}_J = \det G_{*,J}, J = k$
space	$\mathbb{F}^{k \times (n-k)}$	$\mathbb{F}^{\binom{n}{k}}$

Given a generator matrix G of U we can efficiently find a generator matrix H of the dual $U^\perp$

Given a generator matrix G of U we can efficiently find a generator matrix H of the dual $U^\perp$

If $G = [I_k | G']$ is in systematic form, one such generator matrix is $H = [-G'^T | I_{n-k}]$

Given a generator matrix G of U we can efficiently find a generator matrix H of the dual $U^\perp$

If $G = [I_k | G']$ is in systematic form, one such generator matrix is $H = [-G'^T | I_{n-k}]$

Interestingly, if we denote $I^c = [n] \setminus I$, we obtain

$$\det(G_{*,I}) = \pm \det(H_{*,I^c})$$

This suggests defining the following linear operator which is called the Hodge star

$$\begin{aligned}\star : \bigwedge^k \mathbb{F}^n &\rightarrow \bigwedge^{n-k} \mathbb{F}^n \\ \sum_I \alpha_I \mathbf{e}_I &\mapsto \sum_I \pm \alpha_I \mathbf{e}_{I^c}\end{aligned}$$

This suggests defining the following linear operator which is called the Hodge star

$$\begin{aligned}\star : \bigwedge^k \mathbb{F}^n &\rightarrow \bigwedge^{n-k} \mathbb{F}^n \\ \sum_I \alpha_I \mathbf{e}_I &\mapsto \sum_I \pm \alpha_I \mathbf{e}_{I^c}\end{aligned}$$

Together with the last slide, we find

$$\star(\iota(G)) = \iota(H)$$

This suggests defining the following linear operator which is called the Hodge star

$$\begin{aligned}\star : \bigwedge^k \mathbb{F}^n &\rightarrow \bigwedge^{n-k} \mathbb{F}^n \\ \sum_I \alpha_I \mathbf{e}_I &\mapsto \sum_I \pm \alpha_I \mathbf{e}_{I^c}\end{aligned}$$

Together with the last slide, we find

$$\star(\iota(G)) = \iota(H)$$

Thus, if $\mathcal{G}$ is the Plücker embedding of V , then $\star\mathcal{G}$ is the Plücker embedding of $V^\perp$

	Kipnis–Shamir	Plücker
V	$G = [I_k G']$	$\mathcal{G}_J = \det G_{*,J}, J = k$
space	$\mathbb{F}^{k \times (n-k)}$	$\mathbb{F}^{\binom{n}{k}}$
$V^\perp$	$H = [-G'^T I_{n-k}]$	$\star \mathcal{G}$

Let $\mathbf{x} \in \mathbb{F}^n$ be a vector, how do we test whether $\mathbf{x} \in V$?

Let $\mathbf{x} \in \mathbb{F}^n$ be a vector, how do we test whether $\mathbf{x} \in V$?

For generator matrices we simply test $H\mathbf{x} = \mathbf{0}$

Let $\mathbf{x} \in \mathbb{F}^n$ be a vector, how do we test whether $\mathbf{x} \in V$?

For generator matrices we simply test $H\mathbf{x} = \mathbf{0}$

Using maximal minors we can test it by equating the $\binom{n}{k+1}$ maximal minors of

$$\begin{bmatrix} G \\ \mathbf{x} \end{bmatrix}$$

to zero

Let $\mathbf{x} \in \mathbb{F}^n$ be a vector, how do we test whether $\mathbf{x} \in V$?

For generator matrices we simply test $H\mathbf{x} = \mathbf{0}$

Using maximal minors we can test it by equating the $\binom{n}{k+1}$ maximal minors of

$$\begin{bmatrix} G \\ \mathbf{x} \end{bmatrix}$$

to zero

These minors encode exactly the wedge product $\mathcal{G} \wedge \mathbf{x} \in \bigwedge^{k+1} \mathbb{F}_q^n$

	Kipnis–Shamir	Plücker
V	$G = [I_k G']$	$\mathcal{G}_J = \det G_{*,J}, J = k$
space	$\mathbb{F}^{k \times (n-k)}$	$\mathbb{F}^{\binom{n}{k}}$
$V^\perp$	$H = [-G'^T I_{n-k}]$	$\star \mathcal{G}$
$\overset{?}{\mathbf{x}} \in V$	$\langle h_i, \mathbf{x} \rangle = 0 \ \forall i$	$\mathbf{x} \wedge \mathcal{G} = 0$
$\overset{?}{\mathbf{x}} \perp V$	$\langle g_i, \mathbf{x} \rangle = 0 \ \forall i$	$\mathbf{x} \wedge \star \mathcal{G} = 0$

For any $\mathbf{y} \in \mathbb{F}^k$, we get a vector $\mathbf{y}G \in V$

For any $\mathbf{y} \in \mathbb{F}^k$, we get a vector $\mathbf{y}G \in V$

For any subset $I \subset [n]$, $|I| = k - 1$ we get a vector

$$(\pm \mathcal{G}_{I \cup \{1\}}, \dots, \pm \mathcal{G}_{I \cup \{n\}}) \in V$$

For any $\mathbf{y} \in \mathbb{F}^k$, we get a vector $\mathbf{y}G \in V$

For any subset $I \subset [n]$, $|I| = k - 1$ we get a vector

$$(\pm \mathcal{G}_{I \cup \{1\}}, \dots, \pm \mathcal{G}_{I \cup \{n\}}) \in V$$

This vector is the vector $\mathbf{x} \in V$ with $x_{i_1} = \dots = x_{i_{k-1}} = 0$ if it is unique and $\mathbf{0}$ otherwise

Example

Let's construct the vector associated with $\mathcal{G}$ and $I = \{1, \dots, k-1\}$

$$G = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & g_{11} & \cdots & g_{1(n-k)} \\ 0 & 1 & \cdots & 0 & 0 & g_{21} & \cdots & g_{2(n-k)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & 0 & g_{(k-1)1} & \cdots & g_{(k-1)(n-k)} \\ 0 & 0 & \cdots & 0 & 1 & g_{k1} & \cdots & g_{k(n-k)} \end{bmatrix}$$

(

Example

Let's construct the vector associated with $\mathcal{G}$ and $I = \{1, \dots, k-1\}$

$$G = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & g_{11} & \cdots & g_{1(n-k)} \\ 0 & 1 & \cdots & 0 & 0 & g_{21} & \cdots & g_{2(n-k)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & 0 & g_{(k-1)1} & \cdots & g_{(k-1)(n-k)} \\ 0 & 0 & \cdots & 0 & 1 & g_{k1} & \cdots & g_{k(n-k)} \end{bmatrix}$$

$$(0, 0, \dots, 0)$$

Example

Let's construct the vector associated with $\mathcal{G}$ and $I = \{1, \dots, k-1\}$

$$G = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & g_{11} & \cdots & g_{1(n-k)} \\ 0 & 1 & \cdots & 0 & 0 & g_{21} & \cdots & g_{2(n-k)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & 0 & g_{(k-1)1} & \cdots & g_{(k-1)(n-k)} \\ 0 & 0 & \cdots & 0 & 1 & g_{k1} & \cdots & g_{k(n-k)} \end{bmatrix}$$

$$(0, 0, \dots, 0, 1$$

Example

Let's construct the vector associated with $\mathcal{G}$ and $I = \{1, \dots, k-1\}$

$$G = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & g_{11} & \cdots & g_{1(n-k)} \\ 0 & 1 & \cdots & 0 & 0 & g_{21} & \cdots & g_{2(n-k)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & 0 & g_{(k-1)1} & \cdots & g_{(k-1)(n-k)} \\ 0 & 0 & \cdots & 0 & 1 & g_{k1} & \cdots & g_{k(n-k)} \end{bmatrix}$$

$$(0, 0, \dots, 0, 1, g_{k1}$$

Example

Let's construct the vector associated with $\mathcal{G}$ and $I = \{1, \dots, k-1\}$

$$G = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & g_{11} & \cdots & g_{1(n-k)} \\ 0 & 1 & \cdots & 0 & 0 & g_{21} & \cdots & g_{2(n-k)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & 0 & g_{(k-1)1} & \cdots & g_{(k-1)(n-k)} \\ 0 & 0 & \cdots & 0 & 1 & g_{k1} & \cdots & g_{k(n-k)} \end{bmatrix}$$

$$(0, 0, \dots, 0, 1, g_{k1}, g_{k2}, \dots, g_{k(n-k)})$$

In a similar fashion we can sample a -dimensional subspaces

In a similar fashion we can sample a -dimensional subspaces

For a matrix $C \in \mathbb{F}^{a \times k}$ (of rank a), the matrix CG will generate a subspace $W \subset V$

In a similar fashion we can sample a -dimensional subspaces

For a matrix $C \in \mathbb{F}^{a \times k}$ (of rank a), the matrix CG will generate a subspace $W \subset V$

For any subset $J \subset [n], |J| = k - a$ we define

$$\sum_{K \subset [n], |K|=a} \pm \mathcal{G}_{J \cup K} \cdot \mathbf{e}_K$$

In a similar fashion we can sample a -dimensional subspaces

For a matrix $C \in \mathbb{F}^{a \times k}$ (of rank a), the matrix CG will generate a subspace $W \subset V$

For any subset $J \subset [n], |J| = k - a$ we define

$$\sum_{K \subset [n], |K|=a} \pm \mathcal{G}_{J \cup K} \cdot \mathbf{e}_K$$

This is now exactly the Plücker embedding of the subspace defined by

$\mathbf{x}_{j_1} = \dots = \mathbf{x}_{j_{k-a}} = 0$ if it is a -dimensional and $\mathbf{0}$ otherwise

	Kipnis–Shamir	Plücker
V	$G = [I_k G']$	$\mathcal{G}_J = \det G_{*,J}, J = k$
space	$\mathbb{F}^{k \times (n-k)}$	$\mathbb{F}^{\binom{n}{k}}$
$V^\perp$	$H = [-G'^T I_{n-k}]$	$\star \mathcal{G}$
$\overset{?}{\mathbf{x}} \in V$	$\langle h_i, \mathbf{x} \rangle = 0 \ \forall i$	$\mathbf{x} \wedge \mathcal{G} = 0$
$\overset{?}{\mathbf{x}} \perp V$	$\langle g_i, \mathbf{x} \rangle = 0 \ \forall i$	$\mathbf{x} \wedge \star \mathcal{G} = 0$
$\mathbf{x} \in V$	$cG, \quad c \in \mathbb{F}^k$	$(\pm \mathcal{G}_{I \cup \{i\}})_{i \in [n]}, \quad I = k - 1$
$W \subset V$	$CG, \quad C \in \mathbb{F}^{a \times k} \text{ full rank}$	$(\pm \mathcal{G}_{I \cup K})_{ K =a}, \quad I = k - a$

If we sample vectors cG and $c'H$, then by construction $\langle cG, c'H \rangle = 0$

For the Plücker embedding this is not the case!

If we sample vectors cG and $c'H$, then by construction $\langle cG, c'H \rangle = 0$

For the Plücker embedding this is not the case!

If we denote $\mathbf{v}_I$ the vector associated to $\mathcal{G}$ and I and $\mathbf{w}_J$ the vector associated with $\star\mathcal{G}$ and J then

$$\langle \mathbf{v}_I, \mathbf{w}_J \rangle = 0$$

is a non-trivial quadratic equation

If we sample vectors cG and $c'H$, then by construction $\langle cG, c'H \rangle = 0$

For the Plücker embedding this is not the case!

If we denote $\mathbf{v}_I$ the vector associated to $\mathcal{G}$ and I and $\mathbf{w}_J$ the vector associated with $\star\mathcal{G}$ and J then

$$\langle \mathbf{v}_I, \mathbf{w}_J \rangle = 0$$

is a non-trivial quadratic equation

Together* these form the Plücker relations

In practice: MinRank and UOV

For clarity we will use tensor notation in our exposition

We write a matrix M with coefficients M_{ij} as

$$M = \sum_{i,j} M_{ij} \cdot \mathbf{e}_i \otimes \mathbf{e}_j \in \mathbb{F}^m \otimes \mathbb{F}^n \cong \mathbb{F}^{m \times n}$$

For clarity we will use tensor notation in our exposition

We write a matrix M with coefficients M_{ij} as

$$M = \sum_{i,j} M_{ij} \cdot \mathbf{e}_i \otimes \mathbf{e}_j \in \mathbb{F}^m \otimes \mathbb{F}^n \cong \mathbb{F}^{m \times n}$$

Then, a matrix M is of rank r iff there exists $\mathbf{v}_1, \dots, \mathbf{v}_r$ and $\mathbf{w}_1, \dots, \mathbf{w}_r$ such that

$$M = \sum_{i=1}^r \mathbf{v}_i \otimes \mathbf{w}_i$$

Given matrices $M_1, \dots, M_k \in \mathbb{F}^m \otimes \mathbb{F}^n$ find a linear combination of rank r

$$M_\lambda = \sum_{i=1}^k \lambda_i M_i, \quad \text{rank}(M_\lambda) = r$$

Given matrices $M_1, \dots, M_k \in \mathbb{F}^m \otimes \mathbb{F}^n$ find a linear combination of rank r

$$M_\lambda = \sum_{i=1}^k \lambda_i M_i, \quad \text{rank}(M_\lambda) = r$$

We can model the λ_i as indeterminates in the polynomial ring $R = \mathbb{F}[\lambda_1, \dots, \lambda_k]$

Then M_λ is a matrix with coefficients in R

Kipnis-Shamir solved this by modeling the generator matrix $G \in \mathbb{F}^{n-r} \otimes \mathbb{F}^n$ of the right kernel V

In that model we get $k + (n - r) \times r$ variables and equations

$$M_\lambda \cdot G^T = \mathbf{0} \in \mathbb{F}^m \otimes \mathbb{F}^{n-r}$$

Or, if $\mathbf{x}_1, \dots, \mathbf{x}_m$ are the rows of M_λ and $\mathbf{g}_1, \dots, \mathbf{g}_{n-r}$ the rows of G we obtain

$$\sum_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n-r}} \langle \mathbf{x}_i, \mathbf{g}_j \rangle \cdot \mathbf{e}_i \otimes \mathbf{e}_j$$

In other words each row of M_λ should be orthogonal to the kernel V

Thus we can apply the Plücker embedding to V to get $\mathcal{G}$ and test the row vectors there

In other words each row of M_λ should be orthogonal to the kernel V

Thus we can apply the Plücker embedding to V to get $\mathcal{G}$ and test the row vectors there

We obtain the equations $\mathbf{x}_i \wedge \mathcal{G} = \mathbf{0}$ for all $1 \leq i \leq m$

In other words each row of M_λ should be orthogonal to the kernel V

Thus we can apply the Plücker embedding to V to get $\mathcal{G}$ and test the row vectors there

We obtain the equations $\mathbf{x}_i \wedge \mathcal{G} = \mathbf{0}$ for all $1 \leq i \leq m$

This is exactly the Support-Minors model!

Let $v > o$, and m be positive integers and set $n = v + o$. Given matrices $\mathbf{P}_1, \dots, \mathbf{P}_m \in \mathbb{F}_q^{n \times n}$ that vanish on a subspace $O \subset \mathbb{F}_q^n$ of dimension o , find O .

Vanishing means $\mathbf{o}P_i\mathbf{o} = 0$ for all $\mathbf{o} \in O$

This implies that if $\langle \mathbf{v}_1, \dots, \mathbf{v}_v \rangle = O^\perp$, that there exists $\mathbf{w}_i$ and $\mathbf{u}_i$ such that

$$P_i = \sum_j \mathbf{v}_j \otimes \mathbf{w}_j + \sum_j \mathbf{u}_j \otimes \mathbf{v}_j$$

Parametrizing a generator matrix G of the space O , we get the equations

$$\mathbf{g}_r \cdot P_i \cdot \mathbf{g}_s^T = \mathbf{0} \in \mathbb{F}^{o \times o} \quad \forall r, s$$

Equivalently, if $P_i = \sum_j \mathbf{x}_j \otimes \mathbf{y}_j$ we obtain

$$\sum_{j,r,s} \langle \mathbf{g}_r, \mathbf{x}_j \rangle \cdot \langle \mathbf{y}_j, \mathbf{g}_s \rangle \cdot \mathbf{e}_r \otimes \mathbf{e}_s = \mathbf{0}$$

In other words, we are testing orthogonality against either $\mathbf{x}_i$ or $\mathbf{y}_i$

In other words, we are testing orthogonality against either $\mathbf{x}_i$ or $\mathbf{y}_i$

After applying the Plücker embedding we obtain

$$\sum_j (\star \mathcal{G} \wedge \mathbf{x}_i) \cdot (\star \mathcal{G} \wedge \mathbf{y}_i) = \mathbf{0} \in \left(\bigwedge^v \mathbb{F}^n \right)^2$$

In other words, we are testing orthogonality against either $\mathbf{x}_i$ or $\mathbf{y}_i$

After applying the Plücker embedding we obtain

$$\sum_j (\star \mathcal{G} \wedge \mathbf{x}_i) \cdot (\star \mathcal{G} \wedge \mathbf{y}_i) = \mathbf{0} \in \left(\bigwedge^v \mathbb{F}^n \right)^2$$

This is exactly the exterior algebra attack in odd characteristic!

Recap

	Kipnis–Shamir	Plücker
V	$G = [I_k G']$	$\mathcal{G}_J = \det G_{*,J}, J = k$
space	$\mathbb{F}^{k \times (n-k)}$	$\mathbb{F}^{\binom{n}{k}}$
$V^\perp$	$H = [-G'^T I_{n-k}]$	$\star \mathcal{G}$
$\overset{?}{\mathbf{x}} \in V$	$\langle h_i, \mathbf{x} \rangle = 0 \ \forall i$	$\mathbf{x} \wedge \mathcal{G} = 0$
$\overset{?}{\mathbf{x}} \perp V$	$\langle g_i, \mathbf{x} \rangle = 0 \ \forall i$	$\mathbf{x} \wedge \star \mathcal{G} = 0$
$\mathbf{x} \in V$	$cG, \quad c \in \mathbb{F}^k$	$(\pm \mathcal{G}_{I \cup \{i\}})_{i \in [n]}, \quad I = k - 1$
$W \subset V$	$CG, \quad C \in \mathbb{F}^{a \times k} \text{ full rank}$	$(\pm \mathcal{G}_{I \cup K})_{ K =a}, \quad I = k - a$

Thanks for listening!