Optimal 4-dimensional linear codes over $\mathbb{F}_8$

Tatsuya Maruta

Department of Mathematics
and Information Sciences
Osaka Prefecture University
maruta@mi.s.osakafu-u.ac.jp

Overview

We give how to construct new linear codes and how to prove the nonexistence of some codes geometrically to determine $n_8(4, d)$, the minimum value of n for which an $[n, 4, d]_8$ code exists.

Contents

1. Optimal linear codes problem
2. A geometric approach
3. Nonexistence of $[658, 4, 575]_8$ codes
4. Constructing new codes

1. Optimal linear codes problem

$\mathbb{F}_q^n = \{(a_1, a_2, ..., a_n) \mid a_1, ..., a_n \in \mathbb{F}_q\}$.
For $a = (a_1, ..., a_n), b = (b_1, ..., b_n) \in \mathbb{F}_q^n$,
the (Hamming) distance between a and b is

$$d(a, b) = |\{i \mid a_i \neq b_i\}|.$$

The weight of a is $wt(a) = |\{i \mid a_i \neq 0\}| = d(a, \mathbf{0})$.

An $[n, k, d]_q$ code $\mathcal{C}$ means a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum distance d,

$$\begin{aligned} d &= \min\{d(a, b) \mid a \neq b,\ a, b \in \mathcal{C}\} \\ &= \min\{wt(a) \mid wt(a) \neq 0,\ a \in \mathcal{C}\}. \end{aligned}$$

The elements of $\mathcal{C}$ are called codewords.

A good $[n, k, d]_q$ code will have

small n for fast transmission of messages,

large k to enable transmission of a wide variety of messages,

large d to correct many errors.

Optimal linear codes problem.

Optimize one of the parameters n, k, d for given the other two.

Optimal linear codes problem.

Problem 1. Find $n_q(k,d)$, the minimum value of n for which an $[n,k,d]_q$ code exists.

Problem 2. Find $d_q(n,k)$, the largest value of d for which an $[n,k,d]_q$ code exists.

An $[n,k,d]_q$ code is called optimal if

$$n = n_q(k,d) \text{ or } d = d_q(n,k).$$

As for the updated bounds on $d_q(n,k)$ for small q, k, n see the website maintained by Markus Grassl:

http://www.codetables.de/.

Optimal linear codes problem.

Problem 1. Find $n_q(k,d)$, the minimum value of n for which an $[n,k,d]_q$ code exists.

Problem 2. Find $d_q(n,k)$, the largest value of d for which an $[n,k,d]_q$ code exists.

An $[n,k,d]_q$ code is called optimal if

$$n = n_q(k,d) \text{ or } d = d_q(n,k).$$

See also

http://www.geocities.jp/mars39geo/griesmer.htm
for $n_q(k,d)$ tables for some small q and k.

The Griesmer bound

$$n_q(k,d) \geq g_q(k,d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$$

where $\lceil x \rceil$ is a smallest integer $\geq x$.

Griesmer (1960) proved for binary codes.
Solomon and Stiffler (1965) proved for all q.

A linear code attaining the Griesmer bound is called a Griesmer code.
Griesmer codes are optimal.

Problem to determine $n_8(k,d)$ for all d

$[k \leq 4]$

$n_8(k,d) = g_8(k,d)$ for all d for $k = 1, 2$.

$n_8(3,d) = g_8(3,d) + 1$ for

$d =$ 13-16, 29-32, 37-40, 43-48.

$n_8(3,d) = g_8(3,d)$ for other d.

$n_8(4,d)$ is not determined for 488 values of d although $n_8(4,d) = g_8(4,d)$ for all $d \geq 833$, see

R. Kanazawa, T. Maruta, On optimal linear codes over $\mathbb{F}_8$, *Electron. J. Combin.* **18**, #P34, 27pp, 2011.

We consider the following open cases:

$n_8(4,d) = g$ or $g+1$ for $575 \le d \le 608$,

$n_8(4,d) = g+1, g+2$ or $g+3$ for $317 \le d \le 320$,

$n_8(4,d) = g+1$ or $g+2$ for $d = 379, 380, 639, 640$,

where $g = g_8(4,d)$.

Theorem 1. There exist codes with parameters $[368, 4, 320]_8$, $[436, 4, 380]_8$, $[669, 4, 584]_8$, $[678, 4, 592]_8$, $[687, 4, 600]_8$, $[696, 4, 608]_8$, $[733, 4, 640]_8$.

Theorem 2. There exists no $[658, 4, 575]_8$ code.

Corollary.
(1) $n_8(4, d) = g$ for $581 \leq d \leq 608$.
(2) $n_8(4, d) = g{+}1$ for $d = 379, 380, 575, 576, 639, 640$.
(3) $n_8(4, d) = g + 1$ or $g + 2$ for $317 \leq d \leq 320$,

where $g = g_8(4, d)$.

Remark.
$n_8(4, d)$ is still undetermined for 454 values of d.

2. A geometric approach

PG(r,q): projective space of dim. r over $\mathbb{F}_q$

j-flat: j-dim. projective subspace of PG(r,q)

$\theta_j := |\text{PG}(j,q)| = (q^{j+1}-1)/(q-1)$

$\mathcal{C}$: an $[n,k,d]_q$ code with $B_1 = 0$

i.e. with no coordinate which is identically zero

G: a generator matrix of $\mathcal{C}$

The columns of G can be considered as a multiset of n points in $\Sigma = \text{PG}(k-1,q)$ denoted also by $\mathcal{C}$.

$\mathcal{F}_j :=$ the set of j-flats of Σ

$\Sigma \ni P$: i-point $\Leftrightarrow$ P has multiplicity i in $\mathcal{C}$

$\gamma_0 = \max\{i \mid \exists P: \ i\text{-point in } \Sigma\}$

$C_i := \{P \in \Sigma \mid P : i\text{-point}\}$, $0 \leq i \leq \gamma_0$

For $^{\forall}S \subset \Sigma$ we define the multiplicity of S, denoted by $m_{\mathcal{C}}(S)$, as

$$m_{\mathcal{C}}(S) = \sum_{i=1}^{\gamma_0} i \cdot |S \cap C_i|.$$

Then we obtain the partition $\Sigma = \bigcup_{i=0}^{\gamma_0} C_i$ s.t.

$$\begin{aligned} n &= m_{\mathcal{C}}(\Sigma), \\ n - d &= \max\{m_{\mathcal{C}}(\pi) \mid \pi \in \mathcal{F}_{k-2}\}. \end{aligned}$$

Conversely such a partition of Σ as above gives an $[n, k, d]_q$ code in the natural manner.

A line l is called an i-line if $m_{\mathcal{C}}(l) = i$.
An i-plane, an i-hp and so on are defined similarly.

$a_i = |\{H \in \mathcal{F}_{k-2} \mid m_{\mathcal{C}}(H) = i\}| = \#$ of i-hps

List of a_i's: the spectrum of $\mathcal{C}$

Lemma 3. Let Π be an i-hp and let
$t = \max\{|m_{\mathcal{C}}(\Delta)| \mid \Delta \subset \Pi, \Delta \in \mathcal{F}_{k-3}\}$. Then

$$t \le \frac{i + q \cdot (n - d) - n}{q}$$

and an i-hp gives an $[i, k-1, i-t]_q$ code.

For an $[n,k,d]_q$ code $\mathcal{C}$ with a generator matrix G, $\mathcal{C}$ is extendable if $[G,h]$ generates an $[n+1,k,d+1]_q$ code $\mathcal{C}'$ for some column vector h, $h^\top \in \mathbb{F}_q^k$.
$\mathcal{C}'$ is an extension of $\mathcal{C}$.

Theorem 4 (Hill-Lizak, 1999)
$\mathcal{C}$: $[n,k,d]_q$ code, $\gcd(d,q)=1$, $\sum_{i \not\equiv n, n-d \pmod q} a_i = 0$
$\Rightarrow$ $\mathcal{C}$ is extendable.

The nonexistence of $[658,4,575]_8$ codes (Thm 2) is proved applying Thm 4.

3. Nonexistence of $[658, 4, 575]_8$ codes.

Note $n - d = 83$ for $[658, 4, 575]_8$.

Lemma 5
The spectrum of a $[83, 3, 72]_8$ code satisfies $a_i = 0$ for all $i \notin \{3, 5, 7, 9, 11\}$.

An $[n, k, d]_q$ code is called m-divisible if all codewords have weights divisible by an integer $m > 1$.

Theorem (Ward, 2001)
$\mathcal{C}$: a Griesmer $[n, k, d]_8$ code.
If $8|d$, then $\mathcal{C}$ is 2-divisible.

Lemma 6

There exists no $[659, 4, 576]_8$ code.

Proof. $\mathcal{C}_0$: a $[659, 4, 576]_8$ code.

- $a_i = 0$ for all $i \notin \{67, 69, 71, 73, 83\}$.
- $a_{73} = a_{71} = a_{69} = 0$.
- $(a_{67}, a_{83}) = (28, 557)$.

δ: 67-plane.

- δ gives a projective Griesmer $[67, 3, 58]_8$ code.

δ has a 8-line, say ℓ. $x = \#$ of 67-planes through ℓ.

Then $(67 - 8)x + (83 - 8)(9 - x) + 8 = 659$, i.e.,

$y = 15/2$, a contradiction.

Proof of Theorem 2.

$\mathcal{C}$: a $[658, 4, 575]_8$ code.

- $a_i = 0$ for all $i \notin \{66, 67, 68, 69, 70, 71, 72, 73, 82, 83\}$.
- $a_i = 0$ for $67 \le i \le 72$.
- $a_{73} = 0$.
- $a_i = 0$ for all $i \notin \{66, 82, 83\}$, which implies that

$\mathcal{C}$ is extendable by Thm 4 (Hill-Lizak).

This contradicts Lemma 6. □

Open cases

$n_8(4, d) = g_8(4, d)$ or $g_8(4, d) + 1$ for $569 \le d \le 574$.

4. Constructing new codes

An $[n,k,d]_q$ code is called m-divisible if all codewords have weights divisible by an integer $m > 1$.

Lemma 7. $\mathcal{C}$: m-divisible $[n,k,d]_q$ code, $q = p^h$, p prime, $m = p^r$, $1 \leq r < h(k-2)$, $\lambda_0 > 0$, with spec.

$$a_{n-d-im} = \alpha_i \text{ for } 0 \leq i \leq w-1.$$

$\Rightarrow \exists \mathcal{C}^*$: t-divisible $[n^*,k,d^*]_q$ code with $t = q^{k-2}/m$, $n^* = \sum_{j=0}^{w-1} j\alpha_j = ntq - \frac{d}{m}\theta_{k-1}$, $d^* = ((n-d)q-n)t$, whose spectrum is

$$a_{n^*-d^*-it} = \lambda_i \text{ for } 0 \leq i \leq \gamma_0$$

where $\lambda_i = |C_i|$ (# of i-points for $\mathcal{C}$).

$\mathcal{C}^*$ is called a projective dual of $\mathcal{C}$, see

A.E. Brouwer, M. van Eupen, The correspondence between projective codes and 2-weight codes, *Des. Codes Cryptogr.* **11** (1997) 261–266.

Let $\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^6\}$, with $\alpha^3 = \alpha + 1$.
We denote $\alpha, \alpha^2, \cdots, \alpha^6$ by $2, 3, \cdots, 7$ so that $\mathbb{F}_8 = \{0, 1, 2, 3, \cdots, 7\}$.

Lemma 8.
$\mathcal{C}_0$: $[21, 4, 16]_8$ with generator matrix

$$G_0 = \begin{bmatrix} 1&1&1&1&1&1&0&0&1&1&1&1&0&1&1&1&1&1&1&1&1 \\ 6&6&7&4&5&1&1&1&6&6&3&5&1&0&4&4&3&5&2&6&3 \\ 0&6&0&7&0&0&3&3&2&1&7&4&2&5&7&2&1&2&0&3&1 \\ 2&6&3&6&4&7&3&1&2&5&2&3&0&4&0&6&0&5&6&7&2 \end{bmatrix}.$$

$\Rightarrow \mathcal{C}_0$ has spec. $(a_1, a_3, a_5) = (228, 240, 117)$.

As a projective dual of $\mathcal{C}_0$, we obtain a 2^5-divisible $[696, 4, 608]_8$ code $\mathcal{C}$, which is new.

Cor. There exists a $[696, 4, 608]_8$ code with spec. $(a_{56}, a_{88}) = (21, 564)$.

Remark. The code in the previous lemma is from the A. Kohnert's database:

http://www.algorithm.uni-bayreuth.de/en/research/Coding_Theory/Linear_Codes_BKW/

A 4-divisible $[76, 4, 64]_8$ code and a 2-divisible $[28, 4, 22]_8$ code in the database also give new codes with parameters $[368, 4, 320]_8$ and $[733, 4, 640]_8$.

Note: $\mathcal{C}$ is a $[696 = g_8(4,d), 4, d = 608]_8$ code.

To show $\exists[g_8(4,d), 4, d]_3$ codes for $581 \le d \le 608$, it suffices to construct $[g_8(4,d), 4, d]_8$ codes for $d = 584, 592, 600$, 608 since

$$\exists[n,k,d]_q \;\Rightarrow\; \exists[n-1,k,d-1]_q.$$

We construct codes with parameters

$$[687 = g_8(4,d), 6, d = 600]_8$$
$$[678 = g_8(4,d), 6, d = 592]_8$$
$$[669 = g_8(4,d), 6, d = 584]_8$$

applying the following lemma.

Lemma 9.
$\mathcal{C}$: $[n,k,d]_q$ code, $\Sigma = \mathrm{PG}(k-1,q)$, $0 \le t \le k-2$
$\cup_{i=0}^{\gamma_0} C_i$: the partition of Σ obtained from $\mathcal{C}$.
If $\cup_{i\ge 1} C_i \supset \Delta$: t-flat s.t. $(C_1 \setminus \Delta) \cup (\cup_{i\ge 2} C_i)$ spans Σ
$\Rightarrow$ $\exists \mathcal{C}'$: $[n-\theta_t, k, d-q^t]_q$ code

Proof. Define a new partition $\Sigma = \cup_i C_i'$ by

$$C_i' = (C_i \setminus \Delta) \cup (C_{i+1} \cap \Delta) \text{ for all } i$$

which gives an $[n' = n-\theta_t, k, d']_q$ code $\mathcal{C}'$.
For $\forall H \in \mathcal{F}_{k-2}$, $H \cap \Delta = \theta_{t-1}$ or θ_t.
So, $m_{\mathcal{C}'}(H) \le n' - d' \le n - d - \theta_{t-1}$, giving $d' \ge d - q^t$.

Lemma 9.

$\mathcal{C}$: $[n,k,d]_q$ code, $\Sigma = \mathrm{PG}(k-1,q)$, $0 \le t \le k-2$

$\cup_{i=0}^{\gamma_0} C_i$: the partition of Σ obtained from $\mathcal{C}$.

If $\cup_{i\ge 1} C_i \supset \Delta$: t-flat s.t. $(C_1 \setminus \Delta) \cup (\cup_{i\ge 2} C_i)$ spans Σ

$\Rightarrow \quad \exists \mathcal{C}'$: $[n-\theta_t, k, d-q^t]_q$ code

Example.

$\mathcal{C}$: simplex $[\theta_{k-1}, k, q^{k-1}]_q$ code

Δ: a hp of Σ

$\Rightarrow$ $\mathcal{C}'$: Griesmer $[q^{k-1}, k, q^{k-1} - q^{k-2}]_q$ code

Lemma 9.

$\mathcal{C}$: $[n,k,d]_q$ code, $\Sigma = \mathrm{PG}(k-1,q)$, $0 \le t \le k-2$

$\cup_{i=0}^{\gamma_0} C_i$: the partition of Σ obtained from $\mathcal{C}$.

If $\cup_{i\ge 1} C_i \supset \Delta$: t-flat s.t. $(C_1 \setminus \Delta) \cup (\cup_{i\ge 2} C_i)$ spans Σ

$\Rightarrow \quad \exists \mathcal{C}'$: $[n-\theta_t, k, d-q^t]_q$ code

Note.

The converse of Lemma 9 holds if $\exists\Delta$: t-flat s.t.

$m_{\mathcal{C}}(H) \le n-d-\theta_t$ for all hp $H \supset \Delta$.

$\mathcal{C}$: $[696, 4, 608]_8$ with spec. $(a_{56}, a_{88}) = (21, 564)$ found as a projective dual of the $[21, 4, 16]_8$ code $\mathcal{C}_0$.

$C_0 \cup C_1 \cup C_2$: the partition of $\Sigma = \mathrm{PG}(4, 8)$ obtained from $\mathcal{C}$. Then we have

$(\lambda_0, \lambda_1, \lambda_2) = (228, 240, 117)$, where $\lambda_i = |C_i|$.

The sets C_i for $\mathcal{C}$ are given from G_0 in Lemma 8 as follows for $0 \leq i \leq 2$:

$$C_i = \{\mathbf{P}(p_0, \cdots, p_3) \in \Sigma \mid wt(p_0 g_0 + \cdots + p_3 g_3) = 16 + 2i\},$$

where g_i is the $(i + 1)$-th row of G_0 for $0 \leq i \leq 3$.

It can be checked with the aid of a computer that the set $C_1 \cup C_2$ contains three skew lines

$l_1 = \langle 1523, 0152 \rangle$, $l_2 = \langle 2342, 7220 \rangle$, $l_3 = \langle 3545, 5352 \rangle$,

where $x_0x_1x_2x_3$ stands for the point $\mathbf{P}(x_0, \cdots, x_3)$ of Σ.

Applying Lem 9 with $\Pi = l_1$ to $\mathcal{C}$ gives a $[687, 4, 600]_8$ code $\mathcal{C}_1$ with spec. $(a_{55}, a_{79}, a_{87}) = (21, 9, 555)$.

Applying Lem 9 with $\Pi = l_2$ to $\mathcal{C}_1$ gives a $[678, 4, 592]_8$ code $\mathcal{C}_2$ with spec. $(a_{54}, a_{78}, a_{86}) = (21, 18, 546)$.

Applying Lem 9 with $\Pi = l_3$ to $\mathcal{C}_2$ gives a $[669, 4, 584]_8$ code with spec. $(a_{53}, a_{77}, a_{85}) = (21, 27, 537)$.

Lemma 9 can be generalized as follows.

Lemma 10 (Geometric Puncturing).

$\mathcal{C}$: $[n,k,d]_q$ code, $\Sigma = \mathrm{PG}(k-1,q)$, $0 \le t \le k-2$

$\cup_{i=0}^{\gamma_0} C_i$: the partition of Σ obtained from $\mathcal{C}$.

If $\cup_{i\ge 1} C_i \supset \mathcal{F}$: $\{f,m;k-1,q\}$-minihyper

s.t. $(C_1 \setminus \mathcal{F}) \cup (\cup_{i\ge 2} C_i)$ spans Σ

$\Rightarrow$ $\exists \mathcal{C}'$: $[n-f,k,d+m-f]_q$ code

An f-set F in $\mathrm{PG}(r,q)$ is an $\{f,m;r,q\}$-minihyper if

$$m = \min\{|F \cap \pi| \mid \pi \in \mathcal{F}_{r-1}\}.$$

Ex. A line is a $\{q+1,1;r,q\}$-minihyper.

A blocking b-set in some plane is a $\{b,1;r,q\}$-minihyper.

Next, we construct $[436, 4, 380]_8$ from $[449, 4, 392]_8$ by projective puncturing.

Let $\mathcal{H} = \mathbf{V}(x_0x_1 + x_2x_3)$ be a hyperbolic quadric in $\Sigma = \mathrm{PG}(3, 8)$.

Take $P(0010) \in \mathcal{H}$ and $\pi = \mathbf{V}(x_3)$.

(π is the tangent plane at P.)

Putting $C_0 = (\mathcal{H} \cup \pi) \setminus \{P\}$ and $C_1 = \Sigma \setminus C_0$,

one can get a Griesmer $[449, 4, 392]_8$ code, say $\mathcal{C}$.

Note that there is no line in C_1, for $\gamma_1 = 8$.

Instead, we take a blocking 13-set $\mathcal{B}$ in some plane through P as $\mathcal{F}$ in Lemma 10.

Let $\delta = \mathbf{V}(x_0 + x_1)$ and take a blocking 13-set in δ:

$$\mathcal{B} = \{P = 0010, 0011, 0012, 0014, 0017, 1101, 1121, \\ 1161, 1171, 1112, 1132, 1142, 1152\}.$$

Then $\mathcal{B} \subset C_1$. Applying Lemma 10 with $\mathcal{B}$ to $\mathcal{F}$ gives a $[436, 4, 380]_8$ code with spectrum

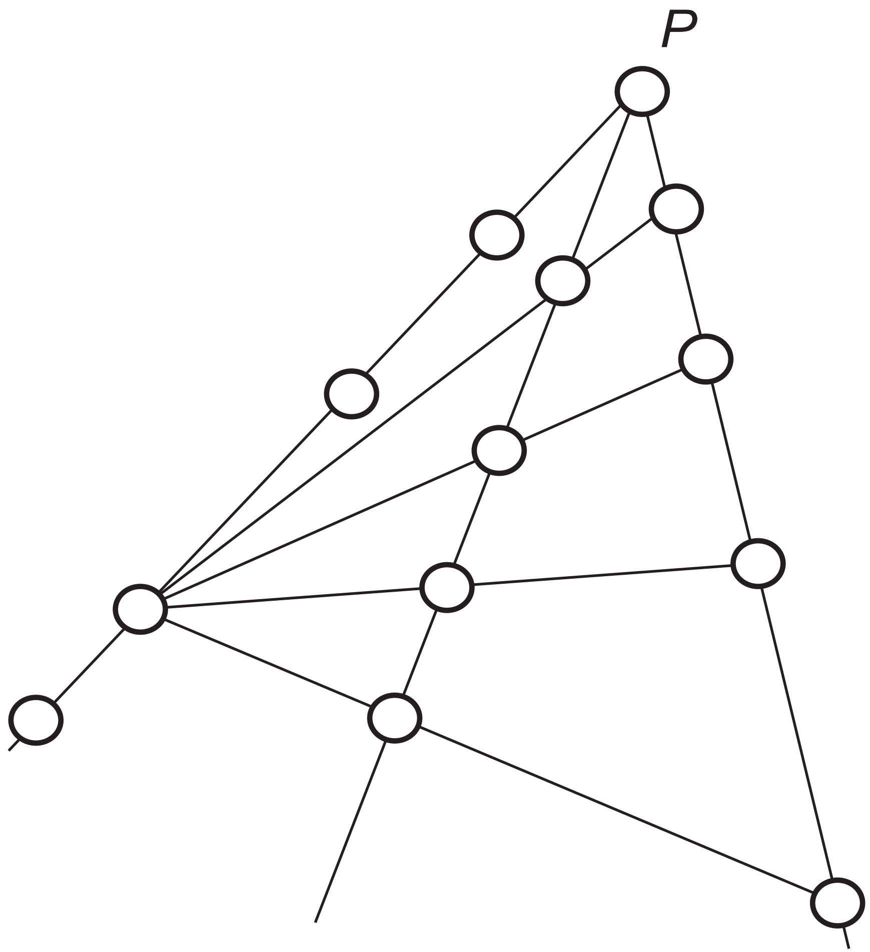
$$(a_0, a_{44}, a_{46}, a_{48}, a_{52}, a_{54}, a_{56}) = (1, 1, 10, 54, 24, 118, 377).$$

This completes the proof of Theorem 1. □

Note: A projective triad of side 5 is a blocking 13-set in PG(2, 8), see

J.W.P. Hirschfeld, Projective Geometries over Finite Fields 2nd ed., Clarendon Press, Oxford (1998).

A projective triad of side 5 in PG(2, 8)



Let $\delta = \mathbf{V}(x_0 + x_1)$ and take a blocking 13-set in δ:

$$\mathcal{B} = \{P = 0010, 0011, 0012, 0014, 0017, 1101, 1121, \\ 1161, 1171, 1112, 1132, 1142, 1152\}.$$

Then $\mathcal{B} \subset C_1$. Applying Lemma 10 with $\mathcal{B}$ to $\mathcal{F}$ gives a $[436, 4, 380]_8$ code with spectrum

$$(a_0, a_{44}, a_{46}, a_{48}, a_{52}, a_{54}, a_{56}) = (1, 1, 10, 54, 24, 118, 377).$$

This completes the proof of Theorem 1. □

Note: A projective triad of side 5 is a blocking 13-set in PG(2, 8), see

J.W.P. Hirschfeld, Projective Geometries over Finite Fields 2nd ed., Clarendon Press, Oxford (1998).

Thank you for your attention!