Monomial clones over $\mathbb{F}_q$

Gábor Horváth, Kamilla Kátai-Urbán and Csaba Szabó

Abstract. The description of the poset of clones generated by a single binary idempotent monomial over $\mathbb{F}_q$ is given by purely number theoretic means.

Mathematics Subject Classification. 08A40, 11A07.

Keywords. finite fields, clone, monomial clone, idempotent clone, congruences, Chinese Remainder Theorem.

1. Introduction

Let q be a prime power and let $\mathbb{F}_q$ denote the q element field. Every n-variable polynomial over $\mathbb{F}_q$ defines a polynomial function over $\mathbb{F}_q$, and every n-variable function is uniquely expressed as an n-variable polynomial of "low" degree. A clone is a subset of functions over $\mathbb{F}_q$ which contains all projections and closed under composition of functions. For more on clone theory, we refer the reader to [1, 2].

As substructures in general, clones over a set S can be ordered with respect to inclusion and they form a partially ordered set. In [5] all binary polynomials are given over the field $\mathbb{F}_3$ that generate a minimal clone. A polynomial will be called a *minimal polynomial* if it generates a minimal clone. In [5] a description of minimal linear polynomials and binary minimal monomials were given. The investigation was extended in [6] to the case of ternary majority minimal polynomials over $\mathbb{F}_3$. Recently in [3] the closed sets of binary monomials were investigated and the corresponding posets over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_5$ were described. The investigation was further developed in [4], where it was shown that over the field $\mathbb{F}_q$ the poset of all closed sets of the unary and binary monomials generated by xy^b is isomorphic to the lattice of divisors of $q-1$. The description of all clones generated by a single binary monomial was formulated as an open problem. In this paper we answer their question (Theorem 4 in Section 2).

The research was supported by the National Research, Development and Innovation Fund of Hungary, financed under the K109185 and FK 124814 funding schemes.

A *binary monomial* over $\mathbb{F}_q$ is a polynomial of the form $x^a y^b$ for some positive integers a, b and the corresponding binary monomial function is $(s;t) \mapsto s^a t^b$ for any $s, t \in \mathbb{F}_q$, as usual. In this paper we shall be interested in binary monomial functions, so for simplicity we write $x^a y^b$ for the function determined by the polynomial $x^a y^b$, as well. Note, that the function $x^a y^b$ over $\mathbb{F}_q$ is the same as $x^{a+q-1} y^b$ or $x^a y^{b+q-1}$, since $x \mapsto x^q$ is the identity function. Therefore, in the paper we mainly will be interested in the modulo $q-1$ residues of the exponents of binary monomials. The modulo $q-1$ residues will be mostly taken from the set $\{1, \ldots, q-1\}$.

A *binary monomial clone* $\mathcal{C}$ contains the functions x, y, and binary monomials such that $\mathcal{C}$ is closed under function composition and permutation of the variables. That is, if $x^a y^{a'}, x^b y^{b'}, x^s y^{s'} \in \mathcal{C}$ for some nonnegative integers a, a', b, b', s, s', then

$$\left(x^a y^{a'}\right)^s \left(x^b y^{b'}\right)^{s'} = x^{as+bs'} y^{a's+b's'} \in \mathcal{C}. \tag{1}$$

Furthermore, if $x^a y^{a'} \in \mathcal{C}$, then $x^{a'} y^a \in \mathcal{C}$ by permuting the variables x and y.

A binary monomial $x^a y^{a'}$ is *idempotent* if substituting the same variable x into every variable we obtain the identity function $x \mapsto x$, that is if $x^a x^{a'} \equiv x$. This happens if and only if $a + a' \equiv 1 \pmod{q-1}$. A *binary idempotent monomial clone* $\mathcal{C}$ is a binary monomial clone $\mathcal{C}$ containing only idempotent binary monomials. Composition of idempotent functions results an idempotent function, as if $a + a' \equiv b + b' \equiv s + s' \equiv 1 \pmod{q-1}$, then $as + bs' + a's + b's' \equiv 1 \pmod{q-1}$, as well. Hence the set of idempotent binary monomials is a clone itself.

In Section 2 we recall some preliminary results, prove some easy propositions, and state the main result (Theorem 4). Then in Section 3 we prove Theorem 4. We finish the paper by posing some open problems in Section 4.

2. Preliminaries

Let $\mathcal{C}$ be an idempotent monomial clone, that is for all $x^a y^{a'} \in \mathcal{C}$ we have $a + a' \equiv 1 \pmod{q-1}$. Let

$$H = \left\{ 1 \le a \le q-1 \mid x^a y^{q-a} \in \mathcal{C} \right\}.$$

Assume $a, b, s \in H$, that is $x^a y^{q-a}, x^b y^{q-b}, x^s y^{q-s} \in \mathcal{C}$. By (1) we have that $x^{as+b(q-s)} y^{(q-a)s+(q-b)(q-s)} \in \mathcal{C}$. Now,

$$as + b(q-s) \equiv as + b(1-s) \pmod{q-1},$$

thus H contains the modulo $q-1$ residue class of $as + b(1-s)$. Furthermore, if $x^a y^{q-a} \in \mathcal{C}$, then by symmetry $x^{q-a} y^a \in \mathcal{C}$, as well. That is, if $a \in H$, then $q - a \equiv 1 - a \in H$. Thus, characterizing all idempotent monomial clones translates to characterize all those subsets $H \subseteq \{1, \ldots, q-1\}$ which have the property that if $a, b, s \in H$, then

$$as + b(1-s) \pmod{q-1} \in H, \tag{2}$$

$$1 - a \pmod{q-1} \in H. \tag{3}$$

Let $S \subseteq \{1, \dots, q-1\}$ be a subset. Then $\langle S \rangle$ denotes the smallest subset of $\{1, \dots, q-1\}$ containing S which is closed under the operations (2–3). The problem posed in [4] was to completely characterize $\langle u \rangle$ for arbitrary $1 \le u \le q-1$.

Example 1. Note that not every clone can be generated by one element. For example, for $q = 31$ the set

$$H = \{1, 6, 10, 15, 16, 21, 25, 30\}$$

is closed under the operations (2–3) modulo 30, but none of its elements generates the whole set. For every $h \in H$ we have $h^2 \equiv h \pmod{30}$, hence each element distinct from 1 and 30 generates a 4 element clone.

The smallest and largest binary monomial clones have already been determined in [4].

Proposition 2 **(**[4, Proposition 5.2]**).** $\langle 2 \rangle = \{1, \dots, q-1\}$.

Proposition 3 **(**[4, Proposition 5.7]**).** *For arbitrary* $1 \le u \le q-1$ *we have* $\{1, q-1\} = \langle 1 \rangle \subseteq \langle u \rangle$.

In the following we give a complete characterization of $\langle u \rangle$ for all $1 \le u \le q-1$ by pure number theoretic means. Note, that operations (2–3) make sense even if q is not a prime power. Therefore, in the following we do not assume that q is a prime power, but only that q is a positive integer and $q > 1$. For convenience, from now on when we write $a \in H$ we mean that the modulo $q-1$ remainder of a from the set $\{1, \dots, q-1\}$ is in H. For example, $q \in H$ means that 1 is in H, and $0 \in H$ means that $q-1$ is in H. Moreover, when we simply write $a \equiv b$ without specifying the module of the congruence, we mean $a \equiv b \pmod{q-1}$.

Throughout the paper we use the notation (a, b) for the greatest (positive) common divisor of the integers a and b. To distinguish from the greatest common divisor, we denote the pair of a and b by putting semicolon in between a and b, i.e. $(a; b)$.

Let $q > 1$ be a positive integer. For our characterization, we will need the following definition. Let $d \mid q-1$ be a divisor, and consider

$$H_d = \{1 \le a \le q-1 \mid a \equiv 0 \text{ or } a \equiv 1 \pmod{d}\}.$$

Then it is easy to check that H_d is closed under the operations (2–3). Note, that $H_1 = H_2 = \{1, 2, \dots, q-1\}$. Our main result is the following.

Theorem 4. *Let* $1 \le u < q$, $d_1 = (u, q-1)$, $d_2 = (1-u, q-1)$. *Then*

$$\langle u \rangle = H_{d_1} \cap H_{d_2}.$$

Example 5. The set of all of the idempotent monomial clones over $\mathbb{F}_{13}$ is $\{\langle 1 \rangle, \langle 2 \rangle, \dots, \langle 6 \rangle\}$. The clones are ordered by inclusion and the structure of this lattice is presented in Figure 1.

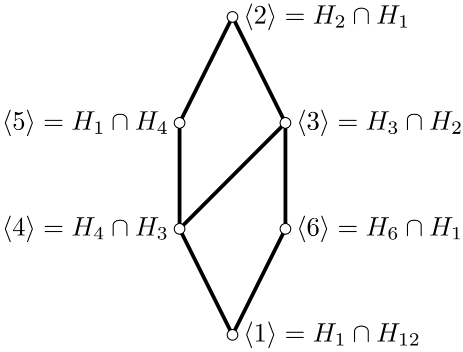

FIGURE 1. Idempotent monomial clones over $\mathbb{F}_{13}$

The following is a very useful property of sets closed under (2–3).

Proposition 6. *Assume $s \in \langle u \rangle$ such that $1 - s$ is invertible modulo $q - 1$. Then for all $t \in \langle u \rangle$ and nonnegative integer k we have that $t + ks \in \langle u \rangle$.*

Proof. Let $H = \langle u \rangle$. We prove Proposition 6 by induction on k. The statement holds for $k = 0$. Assume that the statement holds for $(k-1)$, that is for all $t \in \langle u \rangle$ we have that $t + (k-1)s \in H$. We prove that $t + ks \in H$. Let n be the multiplicative order of $1 - s \pmod{q-1}$, then $(1-s)^{-1} \equiv (1-s)^{n-1}$. Applying (2) with $b = q - 1 \equiv 0$ we obtain that H is closed under multiplication. Hence, $(1-s)^{n-1} \equiv (1-s)^{-1} \in H$. Now, $t + (k-1)s \in H$, and therefore $(t + (k-1)s)(1-s)^{-1} \in H$. Applying (2) with $a = 1$, $b \equiv (t + (k-1)s)(1-s)^{-1}$ shows

$$\begin{aligned} as + b(1-s) &\equiv 1 \cdot s + (t + (k-1)s)(1-s)^{-1}(1-s) \\ &= s + t + (k-1)s = t + ks \in H. \end{aligned}$$

□

We mention the following easy consequence of Proposition 6, which generalizes Proposition 2 and is a special case of Theorem 4.

Corollary 7. *Let $1 \leq u \leq q - 1$ be an integer such that both u and $1 - u$ are invertible modulo $q - 1$. Then $\langle u \rangle = \{1, \ldots, q-1\}$.*

Proof. Let $H = \langle u \rangle$. We prove by induction that for every positive integer k we have $ku \in H$. For $k = 1$ we have $u \in H$. Assume that $ku \in H$ for some positive integer k. Then applying Proposition 6 with $t = ku$ and $s = u$ we obtain that $H \ni t + s = ku + u = (k+1)u$.

Let x be a positive integer solution of the congruence

$$ux \equiv 2 \pmod{q-1}.$$

Such x exists, because u is invertible modulo $q - 1$. Then with $k = x$ we have that $ux \pmod{q-1}$ is in H, that is $2 \in H$. By Proposition 2 we have $H = \{1, 2, \ldots, q-1\}$. □

3. Proof of Theorem 4

Fix $q > u \geq 1$, and let $H = \langle u \rangle$. Since $u \in H_{d_1}$ and $u \in H_{d_2}$, we have $H \subseteq H_{d_1} \cap H_{d_2}$. In the following we prove $H \supseteq H_{d_1} \cap H_{d_2}$

Note, that $(u, 1-u) = 1$, therefore

$$(d_1, d_2) = 1. \tag{4}$$

We need the following about the structure of $H_{d_1} \cap H_{d_2}$.

Lemma 8. *Let $v \in H_{d_1} \cap H_{d_2}$ be arbitrary. Then there exists an integer m and $t \in \{0, 1, u, 1-u\}$ such that*

$$v = t + md_1d_2.$$

In particular, for arbitrary integer k we have $v + kd_1d_2 \in H_{d_1} \cap H_{d_2}$.

Proof. Let $v \in H_{d_1} \cap H_{d_2}$ be arbitrary. We will apply the Chinese remainder theorem. We distinguish four cases depending on the remainder of v by d_1 and by d_2.

$v \equiv 0 \pmod{d_1}$ **and** $v \equiv 0 \pmod{d_2}$**.** By the Chinese remainder theorem, $v \equiv 0 \pmod{d_1d_2}$, and hence there exists an integer m such that $v = md_1d_2$.

$v \equiv 1 \pmod{d_1}$ **and** $v \equiv 1 \pmod{d_2}$**.** By the Chinese remainder theorem, $v \equiv 1 \pmod{d_1d_2}$, and hence there exists an integer m such that $v = 1 + md_1d_2$.

$v \equiv 0 \pmod{d_1}$ **and** $v \equiv 1 \pmod{d_2}$**.** Since $d_1 \mid u$ and $d_2 \mid 1-u$, we have $u \equiv 0 \pmod{d_1}$ and $u \equiv 1 \pmod{d_2}$. By the Chinese remainder theorem, $v \equiv u \pmod{d_1d_2}$, and hence there exists an integer m such that $v = u + md_1d_2$.

$v \equiv 1 \pmod{d_1}$ **and** $v \equiv 0 \pmod{d_2}$**.** Since $d_1 \mid u$ and $d_2 \mid 1-u$, we have $1-u \equiv 1 \pmod{d_1}$ and $1-u \equiv 0 \pmod{d_2}$. By the Chinese remainder theorem, $v \equiv 1-u \pmod{d_1d_2}$, and hence there exists an integer m such that $v = 1-u+md_1d_2$.

□

From (4) we have $(d_1, d_2) = 1$, hence $d_1d_2 \mid q-1$. In the following we prove $H \supseteq H_{d_1} \cap H_{d_2}$ by downward induction on d_1d_2. If $d_1d_2 = q-1$, then $H_{d_1} \cap H_{d_2} = \{0, 1, u, 1-u\}$ by Lemma 8. Since $0, 1, u, 1-u \in H$, we obtain $H_{d_1} \cap H_{d_2} \subseteq H$.

Assume now, that Theorem 4 holds for all pairs $(q-1; v)$ for which the product $(v, q-1) \cdot (1-v, q-1)$ is strictly greater than d_1d_2. Applying (2) with $a = u$, $s = q-u \equiv 1-u$ and $b = q-1 \equiv 0$, we obtain

$$as + b(1-s) \equiv u(1-u) + 0(1-s) = u - u^2 \in H. \tag{5}$$

Since $(u, 1-u) = 1$, we have

$$\begin{aligned}(u-u^2, q-1) &= (u(1-u), q-1) \\ &= (u, q-1) \cdot (1-u, q-1) = d_1d_2.\end{aligned} \tag{6}$$

Applying (3) on (5) we obtain $1-u+u^2 \in H$. Let

$$d_3 = \left(1-u+u^2, q-1\right).$$

Now, $(u, 1-u+u^2) = 1$, thus $(d_1, d_3) = 1$. Similarly, $(1-u, 1-u+u^2) = 1$, thus $(d_2, d_3) = 1$. Furthermore, if $2 \nmid q-1$, then $2 \nmid d_3$, as well. However, if $2 \mid q-1$, then either u or $1-u$ is even, thus $2 \mid d_1 d_2$. Since $(d_1 d_2, d_3) = 1$, we have $2 \nmid d_3$. In any case, $(2, d_3) = 1$. Thus, we have

$$(2d_1 d_2, d_3) = 1. \tag{7}$$

Lemma 9. *If $d_3 = 1$, then $H_{d_1} \cap H_{d_2} \subseteq H$.*

Proof. If $d_3 = 1$, then let m be an arbitrary nonnegative integer, and let x be a positive integer solution of the congruence

$$\left(1-u+u^2\right)\left(u-u^2\right) \cdot x \equiv m d_1 d_2 \pmod{q-1}.$$

Such x exists, because $\left(1-u+u^2, q-1\right) = 1$ and $\left(u-u^2, q-1\right) = d_1 d_2$. By Proposition 6 we obtain that $t + k\left(u-u^2\right) \in H$ for any $t \in H$ and nonnegative integer k. Choosing $k = \left(1-u+u^2\right)x$ and $t \in \{0, 1, u, 1-u\}$ (then $t \in H$) we obtain that $m d_1 d_2$, $1 + m d_1 d_2$, $u + m d_1 d_2$ and $1 - u + m d_1 d_2$ (mod $q-1$) are all in H. Therefore, by Lemma 8 we have $H_{d_1} \cap H_{d_2} \subseteq H$. ☐

Thus, Theorem 4 holds if $d_3 = 1$. In the following we assume $d_3 > 1$. Now, applying (2) with $a = u$, $s = u$ and $b = q - u \equiv 1 - u$ we obtain

$$as + b(1-s) \equiv u^2 + (1-u)^2 = 1 - 2u + 2u^2 \in H. \tag{8}$$

Since $(u - u^2, q-1) = d_1 d_2$, we have

$$\left(2u - 2u^2, q-1\right) \in \{ d_1 d_2, 2 d_1 d_2 \}. \tag{9}$$

Applying (3) on (8) we obtain $2u - 2u^2 \in H$. Let

$$d_4 = \left(1 - 2u + 2u^2, q-1\right).$$

Now, $(u, 1-2u+2u^2) = 1$, thus $(d_1, d_4) = 1$. Furthermore, we have $(1-u, 1-2u+2u^2) = 1$, thus $(d_2, d_4) = 1$. Finally, from $\left(1-u+u^2, 1-2u+2u^2\right) = 1$ we obtain $(d_3, d_4) = 1$. Thus, we have

$$(d_1 d_2 d_3, d_4) = 1. \tag{10}$$

Lemma 10. *If $d_4 = 1$, then $H_{d_1} \cap H_{d_2} \subseteq H$.*

Proof. Let $d_4 = 1$. Applying (2) with $a = u$, $s = u$ and $b = q - 1 \equiv 0$ we obtain $as + b(1-s) \equiv u^2 + 0 \cdot (1-u) = u^2 \in H$. Applying (3) we have $1 - u^2 \in H$. Applying Proposition 6 with $s \equiv 2\left(u - u^2\right)$ we obtain that $t + k\left(2u - 2u^2\right) \in H$ for any $t \in H$ and nonnegative integer k. With the choices of Table 1 we obtain that for all $t \in \{0, 1, u, 1-u\}$ and for every integer l (whether l is even or odd) we have $t + l\left(u - u^2\right) \in H$.

TABLE 1.

t	$\in H$
0	$2k\left(u-u^2\right)$
1	$1+2k\left(u-u^2\right)$
u	$u+2k\left(u-u^2\right)$
$1-u$	$1-u+2k\left(u-u^2\right)$
$u-u^2$	$(2k+1)\left(u-u^2\right)$
$1-u+u^2$	$1+(2k-1)\left(u-u^2\right)$
u^2	$u+(2k-1)\left(u-u^2\right)$
$1-u^2$	$1-u+(2k+1)\left(u-u^2\right)$

Now, let m be an arbitrary nonnegative integer, and let x be a positive integer solution of the congruence

$$\left(1-2u+2u^2\right)\left(u-u^2\right)\cdot x \equiv md_1d_2 \pmod{q-1}.$$

Such x exists, because $\left(1-2u+2u^2, q-1\right)=1$ and $\left(u-u^2, q-1\right)=d_1d_2$. Choosing $l=\left(1-2u+2u^2\right)x$ and $t\in\{0,1,u,1-u\}$ (then $t\in H$) we obtain that md_1d_2, $1+md_1d_2$, $u+md_1d_2$ and $1-u+md_1d_2 \pmod{q-1}$ are all in H. Therefore, by Lemma 8 we have $H_{d_1}\cap H_{d_2}\subseteq H$. □

Thus, Theorem 4 holds if $d_4=1$. In the following we assume $d_4>1$.

Lemma 11. *For every $v\in H$ and for an arbitrary integer l we have $v+l\cdot 2d_1d_2d_4\in H$.*

Proof. Let $v\in H$ be arbitrary, and let l be an arbitrary integer. By (9) we have that $\left(2u-2u^2, q-1\right)$ is either d_1d_2 or $2d_1d_2$. Now, if $\left(2u-2u^2, q-1\right)=2d_1d_2$, then from $d_4>1$ we obtain by induction that $H_{2d_1d_2}\cap H_{d_4}=\left\langle 2u-2u^2\right\rangle\subseteq H$. Choosing $k=l$, Lemma 8 yields that $v+l\cdot 2d_1d_2d_4\in H$.

If $\left(2u-2u^2, q-1\right)=d_1d_2$, then from $d_4>1$ we obtain by induction that $H_{d_1d_2}\cap H_{d_4}=\left\langle 2u-2u^2\right\rangle\subseteq H$. Then choosing $k=2l$, Lemma 8 yields that $v+2l\cdot d_1d_2d_4\in H$. □

Finishing the proof of Theorem 4. Let $t\in\{0,1,u,1-u\}$ be arbitrary, and let m be an arbitrary integer. We prove $t+md_1d_2\in H$, which establishes $H_{d_1}\cap H_{d_2}\subseteq H$ and finishes the proof of Theorem 4. From (10) we have $(d_3,d_4)=1$. From (7) we have $(d_3,2)=1$. Thus $(d_3,2d_4)=1$. Therefore, there exist integers x,y such that

$$xd_3+y2d_4=1.$$

From $d_3>1$ by induction we have $H_{d_1d_2}\cap H_{d_3}=\left\langle u-u^2\right\rangle\subseteq H$. Let

$$v=t+mx\cdot d_1d_2d_3.$$

By choosing $k = mx$, Lemma 8 yields $v \in H_{d_1 d_2} \cap H_{d_3} = \langle u - u^2 \rangle \subseteq H$. By choosing $l = my$, Lemma 11 yields $v + my \cdot 2d_1d_2d_4 \in H$. That is,

$$\begin{aligned} v + my \cdot 2d_1d_2d_4 &= t + mx \cdot d_1d_2d_3 + my \cdot 2d_1d_2d_4 \\ &= t + (xd_3 + 2yd_4) \cdot md_1d_2 = t + md_1d_2 \in H. \end{aligned}$$

Thus, for every $t \in \{0, 1, u, 1-u\}$ and for an arbitrary integer m we have $t + md_1d_2 \in H$, establishing $H_{d_1} \cap H_{d_2} \subseteq H$. Theorem 4 is proved. □

4. Open questions

It looks rather difficult to answer a general question on monomial clones. It does not seem feasible to continue along idempotent clones on several variables before understanding all binary monomial clones.

Problem 1. Find all binary monomial clones over $\mathbb{F}_q$.

The following conjecture could be a good start:

Conjecture 2. *Every binary monomial clone can be obtained as an intersection of some H_d-s.*

Another approach could be to omit monomiality. As every finite clone contains idempotent elements, it makes sense to look for idempotent polynomials in general.

Problem 3. Find all binary idempotent clones over $\mathbb{F}_q$.

References

[1] Csákány, B.: Minimal clones—a minicourse. Algebra Universalis **54**, 73–89 (2005).

[2] Lau, D.: Function algebras on finite sets. Springer Monographs in Mathematics. Springer-Verlag, Berlin (2006). A basic course on many-valued logic and clone theory

[3] Machida, H., Pantović, J.: Monomial clones: local results and global properties. In: 2016 IEEE 46th International Symposium on Multiple-Valued Logic, pp. 78–83. IEEE Computer Soc., Los Alamitos, CA (2016)

[4] Machida, H., Pantović, J.: Three classes of closed sets of monomials. In: 2017 IEEE 47th International Symposium on Multiple-Valued Logic, pp. 100–105. IEEE Computer Soc., Los Alamitos, CA (2017)

[5] Machida, H., Pinsker, M.: Some polynomials generating minimal clones. J. Mult.-Valued Logic Soft Comput. **13**, 353–365 (2007)

[6] Machida, H., Waldhauser, T.: Majority and other polynomials in minimal clones. In: 38th International Symposium on Multiple Valued Logic (ismvl 2008), pp. 38–43 (2008). DOI 10.1109/ISMVL.2008.38

Gábor Horváth
Institute of Mathematics, University of Debrecen, Pf. 400, Debrecen, 4002, Hungary
e-mail, G. Horváth: ghorvath@science.unideb.hu

Kamilla Kátai-Urbán
Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H-6720 Szeged, Hungary
e-mail, K. Kátai-Urbán: katai@math.u-szeged.hu

Csaba Szabó
Eötvös Loránd University, Department of Algebra and Number Theory, 1117 Budapest, Pázmány Péter sétány 1/c, Hungary
e-mail, Cs. Szabó: csaba@cs.elte.hu