Teorija kodiranja in kriptografija 2013/2014

Osnovno o končnih obsegih

Arjana Žitnik

Univerza v Ljubljani, Fakulteta za matematiko in fiziko

Ljubljana, 11. 3. 2014

Grupe

Naj bo G množica in
• dvočlena operacija na G: za vsak par $a, b \in G$ velja $a \bullet b \in G$.

$(G, \bullet)$ je grupa, če

1. je operacija $\bullet$ asociativna:
   $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ za vse $a, b, c \in G$,
2. obstaja enota, tj.
   obstaja element $e \in G$, da velja $e \bullet a = a \bullet e$ za vsak $a \in G$,
3. vsak element ima inverz, tj.
   za vsak $a \in G$ obstaja $b \in G$, da velja $a \bullet b = b \bullet a = e$.
   oznaka za inverz elementa a je a^{-1}

Grupa G je komutativna ali Abelova, če za vsak par $a, b \in G$, velja $(a \bullet b) = (b \bullet a)$.

Primeri grup

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$,
- $(\mathbb{Q}\backslash\{0\}, *)$, $(\mathbb{R}\backslash\{0\}, *)$,
- $(\mathbb{Z}_n, +_n)$,
- $(\mathbb{Z}_n^*, *_n)$.

Red elementa v grupi

Naj bo G končna grupa in $\alpha \in G$.

Definiramo $\alpha^0 = e$ in
$\alpha^i = \underbrace{\alpha \bullet \alpha \bullet \cdots \bullet \alpha}_{i \text{ - krat}}$ za i naravno število.

Red elementa α je najmanjše naravno število s, da je $\alpha^s = e$.
Red elementa α označimo z $\#\alpha$.

Red grupe G je število elementov G, oznaka $|G|$.

Grupa G je ciklična, če vsebje element $\alpha \in G$ reda $|G|$:

$$G = \{\alpha, \alpha^2, \ldots, \alpha^{|G|} = e\}.$$

Eulerjev izrek

Izrek. Naj bo G končna grupa. Potem red elementa $\alpha \in G$ deli red grupe G.

Opomba: če je $\alpha^t = e$, potem lahko zaključimo samo da $\#\alpha$ deli t.

Končni obsegi

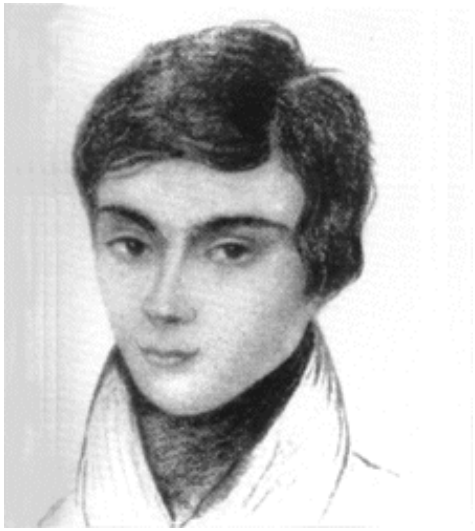
$(K, +, \bullet)$ je obseg, če je

- $(K, +)$ Abelova grupa
- $(K^*, \bullet)$ grupa $\quad (K^* = K \backslash \{0\})$
- velja distributivnost: za vsako trojico a, b, c iz $\mathbb{F}$ je $a \bullet (b + c) = (a \bullet b) + (a \bullet c)$ in $(a + b) \bullet c = (a \bullet c) + (b \bullet c)$.

Torej: znamo seštevati, odštevati, množiti, deliti.

Obseg je končen, če je množica K končna.
Obseg je komutativen, če je grupa $(K^*, \bullet)$ komutativna.

Evariste Galois



Evariste Galois (1811-1832)
je postavil temelje teorije končnih obsegov.

Končen obseg po njem imenujemo Galoisov obseg,
oznaka za končni obseg s q elementi je GF(q).

Praštevilski obsegi

Če je p praštevilo, je $(\mathbb{Z}_p, +_p, \bullet_p)$ končen obseg:

- $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$
- pri seštevanju/množenju običajno vsoto/produkt nadomestimo z ostankom pri deljenju s p.

Primer: $\mathbb{Z}_2$

Naj bo GF(2) $= \mathbb{Z}_2 = \{0, 1\}$.

+	0	1
0	0	1
1	1	0

•	1
1	1

Primer: $\mathbb{Z}_5$

Naj bo GF(5) $= \mathbb{Z}_5 = \{0, 1, 2, 4\}$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

•	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Primer: $\mathbb{Z}_4$ ni obseg

$\mathbb{Z}_4$ s seštevanjem in množenjem po modulu **ni obseg!**
$(\mathbb{Z}_4, +)$ je grupa, vendar $(\mathbb{Z}_4 \setminus \{0\}, \bullet)$ ni grupa.

$\bullet$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Obstoj in enoličnost

- Vsak končen obseg je komutativen.
- Končni obseg GF(q) obstaja le, če je $q = p^m$, kjer je p praštevilo in $m > 0$.
- Obseg GF(q) je en sam, do izomorfizma natančno.
- GF(p^m) ima karakteristiko enako p (tj. za vsak $a \in \mathrm{GF}(p^m)$ je $p \cdot a = 0$).
- Za vsak $a \in \mathrm{GF}(q)$ je $a^q = a$.
- Grupa $(\mathrm{GF}(q)^*, \bullet)$ je ciklična. Njene generatorje imenujemo primitivni elementi oziroma primitivni polinomi.

Velja: $\mathbb{Z}_p$ je končen obseg, če in samo če je p praštevilo.

Konstrukcija obsega GF(p^m)

- Začnemo z obsegom $(\mathbb{Z}_p, +_p, \bullet_p)$
- Vzamemo polinom $f(x)$ stopnje m s koeficienti iz $\mathbb{Z}_p$, ki je nerazcepen nad $\mathbb{Z}_p$.
- Potem je

$$\mathrm{GF}(p^m) = (\{ \text{ polinomi stopnje } < m \text{ s koeficienti iz } \mathbb{Z}_p\}, +_f, \bullet_f),$$

kjer je

- $+_f$ seštevanje polinomov po modulu f (seštejemo običajno, nato vzamemo ostanek pri deljenju s f),
- $\bullet_f$ množenje polinomov po modulu f (množimo običajno, nato vzamemo ostanek pri deljenju s f),

in koeficiente polinomov seštevamo in množimo v $\mathbb{Z}_p$.

Zgled: konstrukcija GF(2^4)

Vzamemo nerazcepen polinom, na primer $f(x) = x^4 + x + 1$

polinom	vektor	polinom	vektor
0	(0000)	$x^3 + x + 1$	(1011)
1	(0001)	$x^2 + 1$	(0101)
x	(0010)	$x^3 + x$	(1010)
x^2	(0100)	$x^2 + x + 1$	(0111)
x^3	(1000)	$x^3 + x^2 + x$	(1110)
$x + 1$	(0011)	$x^3 + x^2 + x + 1$	(1111)
$x^2 + x$	(0110)	$x^3 + x^2 + 1$	(1101)
$x^3 + x^2$	(1100)	$x^3 + 1$	(1001)

Opazimo: element x je generator grupe za množenje!
(To ni vedno res.)

Primer seštevanja in množenja v GF(2^4)

Seštejmo in zmnožimo elementa $x^3 + x + 1$ in $x^2 + x$ (GF(2^4) je generiran z $f(x) = x^4 + x + 1$).

Iskanje inverznega elementa

Poiščimo inverz elementa $x^3 + x^2 + x + 1$ v GF(2^4).
(GF(2^4) je generiran z $f(x) = x^4 + x + 1$).

Uporabimo lahko razširjeni Evklidov algoritem.
Ker je $f(x)$ nerazcepen, bo tuj z vsakim neničelnim polinomom nižje stopnje.

Razširjeni Evklidov algoritem za polinome

Naj bo K obseg in $a(x), b(x) \in K[x]$.
Iščemo polinoma $s(x), t(x) \in K[x]$, da velja

$$s(x)a(x) + t(x)b(x) = \gcd(a(x), b(x)).$$

Uporabimo običajen R.E.A. Postopek se konča, ker je $\deg(r_{i+1}) < \deg(r_i)$ za vsak i.
Dokaz pravilnosti je enak kot pri običajnem R.E.A.