LETNIK 8 (2024) – ŠT. 2 ISSN 2536-3565

Univerza v Mariboru

Fakulteta za naravoslovje
in matematiko

D I A N O I A

REVIJA ZA UPORABO NARAVOSLOVNO-MATEMATIČNIH ZNANOSTI

ISSN **2536-3565**

Naslov publikacije/Title **DIANOIA**, revija za uporabo naravoslovnih in matematičnih znanosti

DIANOIA, journal for applications of natural and mathematical sciences

Letnik/Volume **8**

Leto/Year **2024 (september)**

Številka/Number **2**

Založnik in izdajatelj/ Univerzitetna založba Univerze v Mariboru, Slomškov trg 15, 2000 Maribor, Slovenija,

Published & Issued by http://press.um.si/, zalozba@um.si

Oblikovanje/Design Amadeja Bratuša

Lektoriranje/Proofreading Ljudmila Bokal

Sedež uredništva/Address FNM UM, Koroška cesta 160, 2000 Maribor

e-mail dianoia@um.si

internet/web www.fnm.um.si

Tisk/Printed by FNM UM

Leto izida/Year 2024

Datum natisa/Published 2024

Naklada/Nr. of Copies 100 izvodov

Revija izhaja dvakrat letno, predvidoma aprila in septembra.

Volume 8 Number 2 September 2024

Kazalo / Table of Contents

UVODNIK/EDITORIAL

Dianoia 8 (2024) 65–69

Zelena in digitalna transformacija bosta zaznamovali večino kariere današnjih študentov

Drago Bokal *

Univerza v Mariboru, Fakulteta za naravoslovje in matematiko, Koroška cesta 160, 2000 Maribor

Zelena in digitalna transformacija sta dva pomembna procesa, ki ju izvaja in za prihodnja leta načrtuje evropska politika. Nekoliko poenostavljeno gledano je cilj zelene transformacije do leta 2050 preiti na okoljsko nevtralno gospodarstvo, cilj digitalne transformacije pa je s pomočjo podatkovnih tehnologij, predvsem umetne inteligence, pomagati, da bo ta prehod ohranil konkurenčnost evropskega gospodarstva. Smeli cilji, ki nujno predpostavljajo visoko prilagodljivost in inovativnost gospodarskih subjektov, s tem pa tudi evropskih zaposlenih nosilcev teh sprememb, ki bodo krojile večino kariere tistih, ki so danes že zaposleni, in skoraj vso kariero tistih, ki jih danes izobražujemo.

Univerza v Mariboru pri teh spremembah sodeluje s projektom prilagajanja učnih enot s področja zelenih in digitalnih vsebin. V okviru projekta bo prenovila 64 učnih enot in jih ponudila študentom celotne Univerze kot izbirne vsebine. Na Fakulteti za naravoslovje in matematiko smo k projektu pristopili z osmimi predmeti, torej osmino ponudbe celotne Univerze. Med njimi so bili prilagojeni tudi predmeti Matematično modeliranje, Kombinatorična optimizacija in Operacijske raziskave z matematičnim programiranjem. Njihovo prilagajanje je dalo podlago razmislekom, ki so pripeljali do tega uvodnika.

Poplave, vročinski valovi, mile zime so dejstva, skratka, podnebne spremembe se dogajajo in neracionalno bi bilo to zanikati. Sposobnost prilagajanja nanje je osnovna trajnostnostna kompetenca. K prilagajanju nanje nas spodbuja po eni strani regulativa, po drugi strani pa podatki o škodah, ki jih taki nepredvidljivi dogodki povzročajo. Kot primer prilagajanja lahko navedemo pozebe: zavarovalnice ne zavarujejo več proti pozebi, ker v zadnjih letih pozeba ni negotov dogodek, ampak letna stalnica. Kmetijstvo se bo moralo prilagoditi s spremembo kultur.

Za posameznike regulatorno spodbudo zelene transformacije predstavlja kompetenčni okvir GreenComp, Evropski okvir kompetenc za trajnostnost (Bianchi et al., 2022), regulatorno spodbudo digitalne transformacije pa kompetenčni okvir DigComp 2.2, Okvir digitalnih kompetenc za državljane (Carretero et al., 2022). Priročnika razkrivata pogled stroke in politike na to, kaj morajo posamezniki znati, da bodo lahko sodelovali v zeleni in digitalni transformaciji. Za podjetja je paket še bolj kompleksen. Vrsto regulatornih dokumentov za uvajanje digitalne transformacije je leta 2023 zaokrožila direktiva CSRD

*

E-naslov: drago.bokal@um.si (Drago Bokal)

o trajnostnostnem poročanju (European Commission, 2023), leta 2024 pa so bili na njeni osnovi sprejeti Evropski standardi trajnostnostnega poročanja (European Financial Reporting Advisory Group, 2024). Ti predpisujejo postopno uvajanje več kot tisoč podatkovnih točk v poročanje velikih podjetij v javnem interesu, del kazalnikov pa je tak, da naslavlja tudi dobavitelje teh podjetij. V Sloveniji je takih podjetij nekaj sto, skupaj z dobavitelji pa dosegajo 60 % BDP.

Skupna lastnost vseh regulatornih podlag opisanih procesov je velik obseg z njimi povezane dokumentacije. Zdi se, da ta pomeni eno ključnih ovir pri uresničitvi teh procesov. Kolikokrat ste poslali e-sporočilo in dobili odgovor, da povejte krajše? Koliko študentov je prebralo več kot eno knjigo, ki je navedena v literaturi predmeta? Nujna posledica kompleksnosti problematike je, da je o njej bistveno lažje razpravljati, kot jo izvajati na način, da dá predvidljive rezultate. Po Cynefin kategorizaciji (Snowden, 2007) se namreč vsebina navedene regulative giblje med kaotičnimi (podnebne spremembe) in kompleksnimi (odzivi, o katerih lahko razpravljamo) področji odločanja. Ti nimajo predvidljivih posledic, da bi jih lahko vnaprej analizirali in se na podlagi analiz optimalno odločali. Regulativa pomeni odziv človeštva na opažen kaos nepredvidljivih posledic ravnanja, ki smo ga v preteklosti razvili. Predstavlja možnost, da s ponavljanjem odzivov razvijemo dovolj globoko razumevanje problematike, da bi sčasoma posledice odločitev na teh področjih postale predvidljive.

In ponavljanje teh situacij je zaradi obsega problematike tudi tisto, kar bo prineslo izkušnje tako posameznikom kot podjetjem. Podatki, zbrani v podjetjih s tem ponavljanjem, in izkušnje, ki jih bodo dobili posamezniki, bodo utrdili zavedanje, katere od navedenih vsebin so res pomembne in se je za njihovo uporabo treba opolnomočiti, katere je treba razumeti toliko, da lahko o njih razpravljamo, katere pa lahko preletimo in odložimo, da se jim lahko posvetimo le po potrebi. Posamezniki bodo selekcijo opravili sami, verjetno nezavedno s tem, da se bodo ukvarjali le z vsebinami, na katere bodo naleteli ob delu, v pogovorih, v medijih ali jim bodo zanimive zaradi kakega hobija. Za podjetja pa je izbor relevantnega dela vgrajen v sam začetek procesa trajnostnostnega poročanja, ko morajo pripraviti svojo matriko dvojne bistvenosti (Efrag, 2023).

Druga ključna novost za podjetja pa je revizijska sledljivost dokumentacije za podatke, ki jih navajajo v trajnostnostnem poročilu. Če je bila do nedavnega pomembna predvsem vsebina poročil in morda njihova promocijska vrednost pri strankah in partnerjih, CSRD uvaja revizijo poročil in dokazljivost navedb. Podatkovna in narativna plat dvojnega - zeleno digitalnega prehoda se tako nerazvezno prepletata, regulativa pa bo iz faze spodbujanja zgodnjih uporabnikov (early adopters) k spremembi obnašanja prešla k mandatornim spremembam obnašanja celotnega gospodarstva. Te ne bodo smele biti le kozmetične, kot se je izkazalo pri razvpitem Dieselgate-u (European Parliament, 2019), ampak bodo morale epistemološko zasnovane spremembe obnašanja doseči tudi udejanjanje v ontologiji. Ne bo dovolj imeti dobre strategije - matematičnega modela - kako bodo poslovni procesi podjetja postali okoljsko nevtralni. Potrebno bo tudi dejansko, z revizijsko sledjo izkazati, kako se izmerjene številke ujemajo z načrti.

Eden večjih izzivov okoljske nevtralnosti je gradbeništvo. Za proizvodnjo klasičnega portland cementa se pri žganju apnenca in gline v ozračje spusti skoraj enaka masa ogljikovega dioksida, kot je končna masa proizvoda. Na obisku v Laboratoriju za gradbene materiale UBW München eksperimentirajo z različnimi glinami, apnenci in drugimi materiali. Dosegli so pol manjše izpuste za mešanico, ki pri izbranih pogojih doseže enake rezultate trdnosti betona kot portland cement (Slika 1). Ko bo v partnerskem podjetju raz-

vita industrijska proizvodnja te mešanice in bo le-ta certificirana za uporabo v betonarnah, bo mešanica postala najboljša razpoložljiva tehnologija. Regulativa o uporabi najboljših razpoložljivih tehnologij (European Commission, 2021) bo poskrbela, da bo njena uporaba v izbranih pogojih izpodrinila sicer cenejši in univerzalno uporaben, a okoljsko bistveno bolj tvegan portland cement. Matematično gre sicer za večkriterijsko optimizacijo, ki poleg kriteriju okoljske obremenjenosti, sledi tudi kriterijem kakovostne ustreznosti in ekonomske upravičenosti, kar odpira priložnosti novih poslovnih niš, a ključno je, da vsi deležniki razumejo in opravijo svojo vlogo v procesu. Profesor Thienel, ki je s ponosom razkazal svoje dosežke, je izgubljal le malo besed o regulativi in drugih epistemoloških elementih zelene transformacije: on počne to, kar ga najbolj veseli. V laboratoriju, ki je zasnovan kot prava cementarna z betonarno, razvija cementne mešanice, ki dajejo čim trdnejši beton ob čim manjših emisijah toplogrednih plinov. Njegovi študentje bodo med študijem to tehnologijo usvojili in jo prenesli na njihova delovna mesta, s čimer bodo v kombinaciji z BAT regulativo dvignili konkurenčnost svojih delodajalcev.

Slika 1: Prepolovitev ogljičnega odtisa portlant cementa. Vir: lasten

Drugi od sedemnajstih trajnostnostnih ciljev Združenih narodov je čista voda (United Nations, n.d.). Na oddelku za upravljanje z urbanimi vodami in s tehnologijo odpadkov taiste univerze so prikazali zanimivo kombinacijo zelene in digitalne transformacije: dva zabojnika, v katerih deluje z raznovrstno digitalno senzoriko opremljena čistilna naprava, ki prečiščuje vse odpadne vode univerzitetnega kampusa. S pomočjo senzorjev merijo kakovostne parametre vode, z aktuatorji dozirajo reagente za izboljševanje kakovosti vode, digitalni dvojček celotnega procesa pa modelira povezavo med parametri kakovosti nečiste vode, doziranjem reagentov in drugimi parametri na upravljani strani čistilnega procesa ter izmerjenimi parametri očiščene vode na izhodni strani procesa. Partnersko podjetje, ki jim je razvilo gradnike tehnologije, ima preko projektov, v katerih sodelujejo, dostop do podatkov in modelov. Študenti se v okviru rednega pouka izobražujejo, kako upravljati aktualne

čistilne naprave, na digitalnem dvojčku pa spoznavajo smeri, v katere se bo tehnologija razvila in to znanje prenesejo v industrijo.

Če gornja dva primera nakazujeta idealiziran primer prenosa znanja iz laboratorija v prakso, pa je morda smiselno omeniti še primer, ki trajnostnostno ni optimalen. Nedavno je Talum iz Kidričevega ustavil proizvodnjo primarnega aluminija, kljub temu da je bil ogljični odtis njihove proizvodnje za večkrat nižji kot ogljični odtis konkurenčnega primarnega aluminija iz azijskih držav. Nestabilne cene električne energije v prejšnjem letu so povzročile, da proizvodnja cenovno ni bila konkurenčna, čeprav je snovanje procesne optimizacije, ki je ogljični odtis nižala, ob predpostavljenih cenah zagotavlja smiselnost sprememb. Primer lahko smatramo kot opozorilo, da optimizacija procesov vodi le-te iz neke cone udobja proti mejam njihove izvedljivosti, ki terjajo ali večjo kakovost podatkov oz. stabilnost napovedi ali večjo odpornost proti tveganjem. Ustrezni digitalni modeli procesov lahko tovrstna tveganja predvidijo in upoštevajo pri analizah odločitev.

Kako naj torej povzamemo predstavljene izzive in primere evropskega dvojnega - zelenega in digitalnega - prehoda? Kot prvo, zavedati se je treba, da receptov za te naloge ni in vsako podjetje in verjetno tudi posameznik bodo morali poiskati sebi lastno pot. Posledice strateških odločitev na tej poti so nepredvidljive. Deloma lahko z napredno podatkovno analizo iz dovolj velikega podatkovnega nabora pridemo do intervalnih ocen tveganj, bistveno pa bi gospodarstvu pomagalo, če bi razumevanje tveganega dela prehodnih procesov znali ovrednotiti ali morda celo obvladati v manj tveganem akademskem okolju. Kot že omenjeno, smo v okviru prilagajanja učnih enot s področja zelenih in digitalnih vsebin prilagodili tudi predmete Matematično modeliranje, Kombinatorična optimizacija in Operacijske raziskave z matematičnim programiranjem. V sklopu prilagajanja smo poleg uvajanja dodatnih vsebin povezanih z zeleno transformacijo, v skladu z novostmi na področju visokošolske didaktik,e posodobili tudi način dela s sodobnimi učnimi pristopi, kot na primer ‘obrnjena učilnica’ ter alternativnimi metodami ocenjevanja znanja, kot na primer projektno delo. Tu pa je priložnost za študente, ki želijo preseči klasično reševanje kolokvijev in opravljanje izpitov: z zavestjo, da noben življenjsko relevanten problem ni po enostavnosti primerljiv z izpitnimi nalogami, lahko posežejo po izzivih, ki bodo krojili prihajajoča desetletja njihove kariere in se pripravijo za izzive, za katere tudi delodajalci trenutno še zgolj slutijo, da prihajajo.

Literatura

[1] Bianchi, G., Pisiotis, U., & Cabrera Giraldez, M. (2022). GreenComp: The European sustainability competence framework. Publications Office of the European Union.

[2] Carretero, S., Vuorikari, R., Punie, Y., & Castaño-Muñoz, J. (2022). DigComp 2.2: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use. Publications Office of the European Union.

[3] European Commission. (2021). Best Available Techniques (BAT) Reference Documents.

[4] European Commission. (2023). Corporate Sustainability Reporting Directive (CSRD).

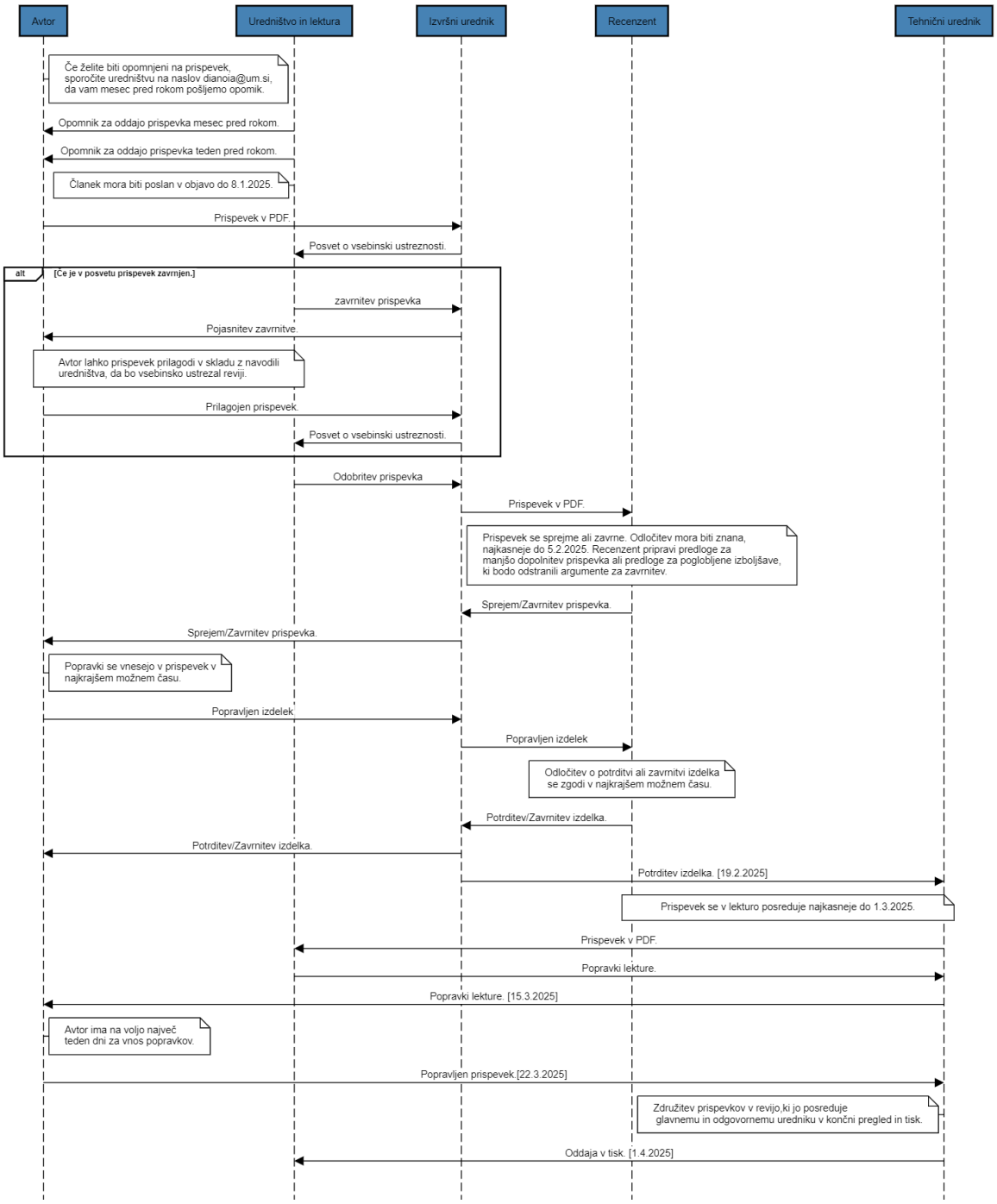
[5] European Financial Reporting Advisory Group (EFRAG). (2023). ESRS Implementation Guidance on Double Materiality.

[6] European Financial Reporting Advisory Group (EFRAG). (2024). European Sustainability Reporting Standards (ESRS).

[7] European Parliament. (2019). Dieselgate: A Major Scandal That Opened the Door to Greater EU Control.

[8] United Nations (b.d.). Sustainable Development Goals.

[9] Snowden, D. J., Boone, M. E. (2007). A Leader's Framework for Decision Making, Harvard Business Review, 85, 68-76.



Slika 2: Proces izdaje naslednje številke Dianoia. Vir:lasten

Dianoia 8 (2024) 71-78

Merjenje naboja na prevodni krogli

Measuring charge on a conductive sphere

Alen Labohar[1], Tjaš Esih[1], Jure Šantej[1], Mitja Suvajac[2]

1. *Gimnazija Celje-Center*
2. *Fakulteta za naravoslovje in matematiko, Univerza v Mariboru*

Povzetek

V prispevku obravnavamo merjenje naboja na prevodni krogli, ki visi na neprevodni nitki v homogenem električnem polju, z meritvijo kota odmika nitke od navpičnice. Naloga je bila podana kot eden izmed problemov na tekmovanju IYPT 2024. Cilj naloge je raziskati zanesljivost in natančnost meritev, narejenih po takšni metodi. V članku obravnavamo eksperiment in analiziramo merske napake. Pokažemo, da je napaka izmerjenega naboja 10 %, če so koti odmika večji od 3,0°. Z uporabljeno grafitno kroglo lahko merimo električni naboj reda velikosti 10 nC s približno 10 % napako, pri naboju reda velikosti 1 nC pa je napaka že 20 %. Manjše naboje bi lahko merili z večjo zanesljivostjo, če bi imeli prevodno kroglo z manjšo maso in polmerom.

Ključne besede: IYPT, merilnik naboja, prevodna sfera, Coulombova sila, ImageJ

Abstract

In this paper, we discuss the measurement of the charge on a conductive sphere suspended by an insulating thread in a homogeneous electric field, by observing the angle of deflection of the thread from the vertical. This task was presented as one of the problems in the IYPT 2024 competition. The objective of the task is to investigate the reliability and accuracy of measurements made using this method. We present the experiment and analyse the measurement errors. We demonstrate that the error of the measured charge is 10% if the deflection angles are greater than 3.0°. Using the employed graphite sphere, we can measure an electric charge of the order of 10 nC with approximately 10% error, while for a charge of the order of 1 nC, the error is already 20%. Smaller charges could be measured with greater reliability if we had a conductive sphere with a smaller mass and radius.

Key words: IYPT, charge meter, conductive sphere, Coulomb force, ImageJ

1 UVOD

Prvi trije avtorji tega prispevka se pod vodstvom zadnjega avtorja že vrsto let udeležujemo Mednarodnega turnirja mladih fizikov IYPT (angl. International Young Physicists' Tournament), ki temelji na samostojnem raziskovanju vnaprej izbranih fizikalnih problemov, pri katerih se pričakuje podrobno povezovanje teoretičnih napovedi z eksperimentalnimi rezultati in njihova predstavitev[1]. Turnir je namenjen predvsem dijakom srednjih šol, ki si želijo podrobneje spoznati utrip raziskovalnega dela.

Turnirja se udeležujemo zaradi našega zanimanja za fiziko in njegove narave samostojnega, znanstvenega postopka dela, kar nam ponuja seznanitev s pristnim načinom znanstvenega raziskovanja. Problemi IYPT so pogosto kompleksni in večinoma zahtevajo poglobljeno znanje na področjih mehanike, elektromagnetizma, hidrodinamike, optike idr. Ta področja se pogosto medsebojno prepletajo ter se s tem približajo realnim fizikalnim problemom.

Med temami proučevanja, ki so bile razpisane za IYPT 2024, je tudi tema tega prispevka, in sicer problem številka trinajst, Merilnik naboja (angl. Charge Meter). Naloga navede, da se naelektrena prevodna krogla, ki je obešena med dvema kovinskima ploščama z različnima električnima potencialoma, odkloni proti nasprotno naelektreni plošči. Od raziskovalca zahteva meritev naboja na krogli preko kota odklona nitke od navpičnice in oceno natančnosti meritev. Prav tako sprašuje po najmanjšem naboju, ki se lahko izmeri na takšen način[2]. Problem je podoben principu Franklinovih zvonov[3] in elektrostatičnega nihala, kot ga opisuje Vladimir A. Saranin[4], le da se ne osredotoča na nihanje prevodne krogle med ploščama oziroma zvonovoma, temveč na stanje mehanskega ravnovesja sil, ki delujejo na naelektreno kroglico.

E-mail naslov: mitja.suvajac@sic-alma.si (Mitja Suvajac)

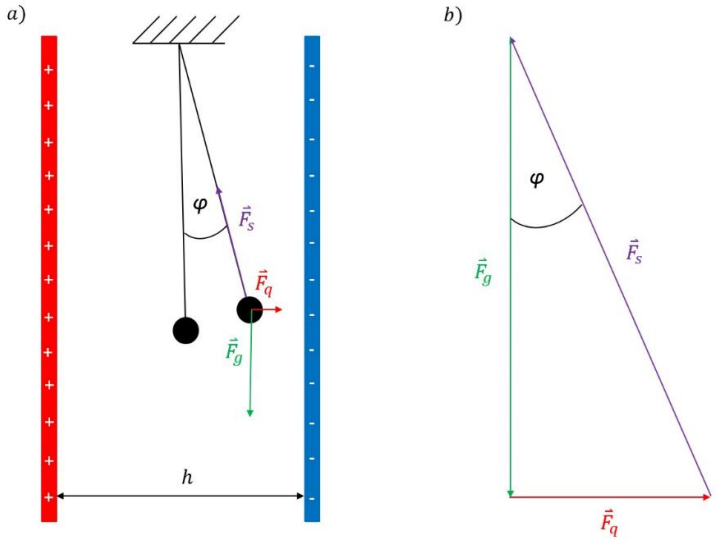
V nadaljevanju najprej predstavimo, kako naboj na krogli ocenimo iz električnega potenciala krogle in kako iz meritve kota odklona nitke. Nato opišemo postavitev eksperimenta in merilni sistem ter podamo rezultate meritev kota odklona v odvisnosti od polmera in mase krogle, naboja na krogli, razdalje med kovinskima ploščama in napetosti med njima.

2 METODE OCENE NABOJA

V obravnavanem problemu je opazovani sistem krogla, ki na tanki neprevodni nitki visi med dvema kovinskima ploščama, na katerih z generatorjem enosmerne napetosti vzpostavimo različna električna potenciala in tako med njima ustvarimo homogeno električno polje (slika 1). Sicer naelektrena krogla povzroča tudi lastno električno polje, vendar predpostavimo, da je slednje prešibko, da bi spremenilo homogeno polje zaradi naboja na kovinskih ploščah. Predpostavimo tudi, da na površini krogle ni deformacij in da je naboj enakomerno porazdeljen po površini.
Kroglico naelektrimo tako, da na generatorju enosmerne napetosti nastavimo neko napetost U in se nato z vezno žico, ki je na eni strani priključena v generator, dotaknemo površine krogle. Ker poznamo napetost na krogli in njen polmer, lahko iz tega ocenimo, kolikšen je naboj na površini krogle. Namreč, kroglo, kjer je električni naboj q enakomerno porazdeljen po površini, lahko obravnavamo kot točkasti naboj, ki ga postavimo v središče krogle. Električni potencial (ϕ_e) točkastega naboja na oddaljenosti r od naboja je $\phi_e = q/(4\pi\varepsilon_0 r)$, kjer je ε_0 influenčna konstanta. Ker vemo, da je na oddaljenosti polmera krogle (R) potencial enak napetosti U, lahko izrazimo naboj na površini krogle kot

$$q = 4\pi\varepsilon_0 RU\,. \tag{1}$$

Sedaj pa poglejmo, kako je kot odklona nitke od navpičnice odvisen od velikosti naboja na krogli, ko krogla visi med naelektrenima kovinskima ploščama.



Slika 1. a) Naelektrena prevodna krogla med naelektrenima kovinskima ploščama, ki sta na razdalji h. Če je krogla naelektrena s pozitivnim nabojem, se primakne k negativno naelektreni kovinski plošči, tako da vrvica z navpičnico oklepa kot φ. Na kroglo delujejo sila nitke ($\vec{F}_s$), sila teže oz. gravitacijska sila ($\vec{F}_g$) in električna sila ($\vec{F}_q$). b) V ravnovesni legi je vsota vseh treh sil enaka 0.

Na kroglo, ki visi na nitki, v zunanjem električnem polju delujejo tri sile: sila nitke ($\vec{F}_s$), sila teže oz. gravitacijska sila ($\vec{F}_g$) in električna sila ($\vec{F}_q$). Ko je krogla v ravnovesni legi (lega (2) na sliki 1a), je vsota vseh sil, ki delujejo nanjo, enaka 0:

$$\vec{F}_g + \vec{F}_s + \vec{F}_q = 0 \ , \tag{2}$$

kar je grafično prikazano na sliki 1b. Iz slike 1b razberemo zvezo med gravitacijsko in električno silo:

$$\mathrm{tg}(\varphi) = \frac{F_q}{F_g} \ , \tag{3}$$

kjer je φ odklon nitke od navpičnice. Električno silo izračunamo tako, da naboj na krogli obravnavamo kot točkasti naboj. Velikost sile na električni naboj (q) v električnem polju z jakostjo E je $F_q = qE$, jakost električnega polja pa izračunamo iz napetosti med kovinskima ploščama (U_p) in razdalje med njima (h) kot $E = U_p/h$. Upoštevamo še, da je $F_g = mg$, kjer je m masa krogle in g težni pospešek, in enačbo (3) zapišemo kot

$$\mathrm{tg}(\varphi) = \frac{qU_p}{mgh} \ . \tag{4}$$

V primeru, da so koti odklona majhni, pa lahko upoštevamo še približek $\mathrm{tg}(\varphi) \approx \varphi$ in dobimo izraz

$$\varphi \approx \frac{qU_p}{mgh} \ , \tag{5}$$

od koder se vidi, da so koti odklona večji pri višji napetosti med ploščama, manjši razdalji med njima, večjem naboju na krogli ter manjši masi krogle. Iz enačbe (4) lahko izrazimo naboj na krogli:

$$q = \frac{mgh\ \mathrm{tg}(\varphi)}{U_p} \ . \tag{6}$$

Naboj, izračunan po enačbi (1), nato primerjamo z nabojem, ki ga dobimo z merjenjem odklona nitke, ko je naelektrena krogla v homogenem električnem polju (enačba (6)).

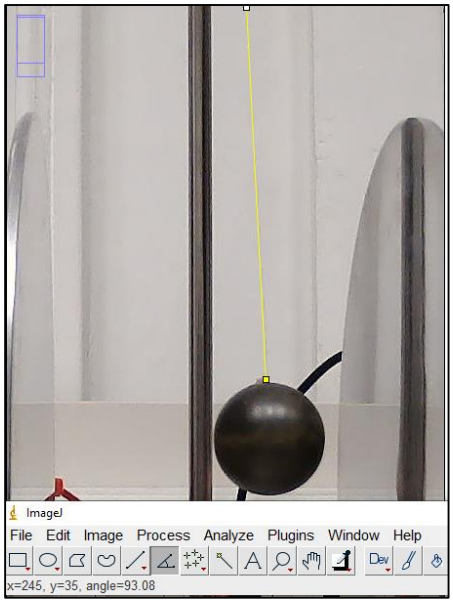
Moramo še poudariti, da ima opisana metoda določene pomanjkljivosti, saj ne upošteva razelektritve krogle zaradi naelektrenih delcev v zraku, prav tako ne predvidi, kako neposredna bližina naelektrene plošče vpliva na velikost odklona.

3 EKSPERIMENTALNI DEL

Eksperiment za oceno naboja na krogli iz meritve kota odklona nitke, na kateri visi krogla, smo zastavili tako, da smo lahko spreminjali polmer in maso krogle, naboj na krogli, napetost med kovinskima ploščama in razdaljo med njima. Uporabljen pribor ločimo na eksperimentalnega in merilnega. Eksperimentalni vključuje vse pripomočke za postavitev eksperimenta, merilni pa pripomočke, s katerimi smo izmerili fizikalne lastnosti eksperimentalnega pribora in kot odklona.

3.1 Merilni pribor

Pri meritvah smo kot merilne pripomočke uporabljali pomično in kovinsko ravnilo, tehtnico, kamero z ločljivostjo 1920 x 1080 pik ter računalniška programa ImageJ[5] in Excel. Kamero smo pritrdili na razdalji 40 cm od eksperimentalnega pribora in jo poravnali z navpično lego nitke, kar je ob majhnih kotih odklona zadoščalo, da na rezultatih ni bil viden vpliv paralakse. Pri vsaki meritvi smo naredili dve sliki, eno, v kateri je vrvica navpična, in drugo, kjer je odklonjena. S programom ImageJ smo nato na slikah izmerili kot med vrvico in vodoravnico. Slednjo določa program in je vzporedna z robom slike (gl. sliko 2). Ta kot smo odšteli od 90° in dobili velikosti kota odklona φ. Vse meritve smo beležili in obdelovali z Excelom.



Slika 2: Primer merjenja kota odklona s fotografije z računalniškim programom ImageJ. Program odčita kot (v tem primeru 93,08°) med vrvico in vodoravnico, ki je vzporedna s spodnjim robom slike.

3.2 Eksperimentalni pribor

Za potrebe eksperimenta smo izdelali set krogel iz aluminijaste folije, ki smo jo potlačili do krogelne oblike. Tako na enostaven način dobimo večje število krogel z različnim polmerom in maso. Izdelali smo tri krogle z različnimi polmeri (preglednica 1), ki smo jih uporabili za preizkušanje odvisnosti kota odklona od mase (glej enačbo (5)). Izkazalo se je, da so tako izdelane krogle polne ostrih robov in deformacij na površini, zato so neuporabne za ocene nabojev na njih. Poskus smo zato izvedli še z votlo grafitno kroglo, ki ima gladko površino, brez vidnih nepravilnosti. Masa grafitne krogle je bila dovolj velika, da smo lahko zanemarili maso nitke, na kateri je krogla visela (preglednica 1). Pri vseh meritvah smo krogle postavljali na polovično razdaljo med ploščama in tako povečali njihovo konsistentnost.
Kovinski plošči, vsaka s polmerom $(12{,}4 \pm 0{,}1)$ cm, sta bili pritrjeni na neprevodne nosilce. Razdaljo med ploščama, ki smo jo lahko nastavljali od 0 do 23 cm, smo odčitali na vgrajenem ravnilu.
Za nanašanje električnega naboja na plošče in krogle smo uporabili generator enosmerne napetosti z razponom od 0 do 25,3 kV.

Plašč	Material	R [mm]	m [g]	l [cm]	μ [g cm^{-1}]	m_s [g]
robat	aluminij	3,85	0,07	18	0,012	0,29
		5,20	0,17	18	0,012	0,39
		6,41	0,31	18	0,012	0,53
gladek	grafit	18,67	1,40	/	zanemarljiva	1,40

Preglednica 1: Podatki o uporabljenih kroglah in nitkah; R je polmer krogle in m njena masa, l je dolžina nitke z linearno gostoto μ in m_s skupna masa nitke in krogle.

3.3 Odvisne in neodvisne spremenljivke

Za neodvisne spremenljivke smo izbrali razdaljo med ploščama, napetost med njima, napetost generatorja, s katero naelektrimo kroglo, in maso krogle. Odvisna spremenljivka je samo kot odmika nitke od navpičnice, z meritvijo katerega ocenimo naboj na krogli.

4 REZULTATI IN ANALIZA

Opravljene meritve razdelimo v dve skupini. V prvi smo preverjali odvisnost kota odklona od napetosti med kovinskima ploščama, razdalje med njima, mase krogle in napetosti, s katero naelektrimo kroglo. Velikost kota odklona je pomembna zaradi narave merilnega postopka, ki zahteva optično zaznavo spremembe naklona nitke, na kateri visi krogla. Želeli smo določiti najbolj optimalne pogoje za merjenje naboja na krogli velikostnega reda 10^{-9} C. V drugi skupini meritev smo merili kot odklona in iz meritev ocenili naboj na krogli. Tukaj smo uporabili le grafitno kroglo. Rezultate smo nato primerjali z nabojem, ki ga izračunamo po enačbi (1) iz napetosti generatorja, s katero smo naelektrili kroglo.

4.1 Analiza napake

Vse meritve so zaznamovane z napako in naše niso nikakršna izjema. Glavna napaka izvira iz postopka naelektritve krogle in kovinskih plošč. Kroglo naelektrimo tako, da se najprej z vodnikom, ki je povezan na ozemljen izhod generatorja enosmerne napetosti, dotaknemo prevodne krogle. S tem nastavimo relativno »potencialno ničlo« na krogli. Nato se je ponovno dotaknemo še z vodnikom iz drugega izhoda generatorja in tako na krogli ustvarimo želen električni potencial. Nato vodnika iz izhoda generatorja enosmerne napetosti priključimo na kovinski plošči. Potem postopno večamo razliko potencialov med ploščama do želene vrednosti. Pri tem se neizogibno pojavi rahlo nihanje krogle zaradi neenakomernega večanja električne sile na kroglo. Slednje je bolj očitno pri večjih kotih odmika. Napako zaradi nihanja smo dodali k sistematični napaki zaradi odčitka kota.

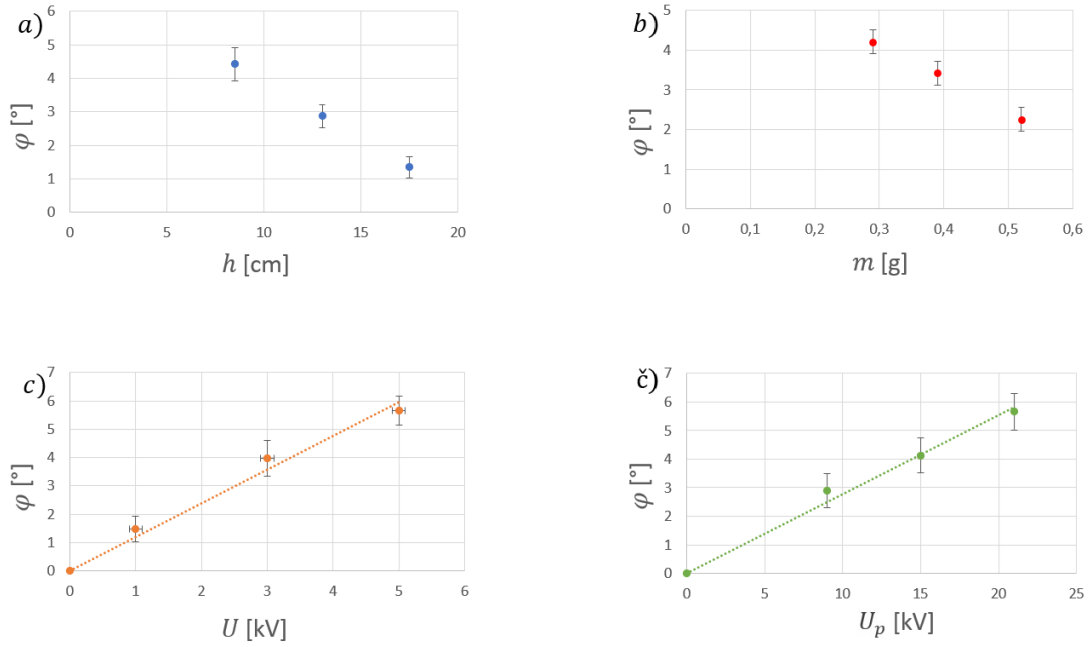
Natančnost odčitka kota je omejena z resolucijo zajetih slik, saj se vrv na slikah razpne čez tri slikovne elemente in zaradi zamegljene podobe ni možno določiti njene natančne lege. Absolutno napako kota tako ocenjujemo na $\pm 0{,}2°$, zato je meritev manjših kotov zaznamovana z večjo relativno napako.

Pri določanju naboja na krogli upoštevamo napako generatorja enosmerne napetosti, ki jo zaradi analogne skale ocenjujemo na ± 10 V. Kroglo naelektrimo s priključkom na napetost od 0,1 kV do 3,0 kV, tako da ima ta napaka največjo vrednost 10 % (preglednica (2)).

Napake zaradi meritve mase in polmera krogle so za več kot velikostni red manjše od navedenih, zato jih ne upoštevamo pri oceni končne napake.

4.2 Meritve

V 2. poglavju smo pokazali, da je kot odklona pri majhnih kotih ($\varphi < 10°$) premo sorazmeren z napetostjo med kovinskima ploščama in napetostjo, s katero smo kroglo naelektrili, ter obratno sorazmeren z maso krogle in razdaljo med ploščama. Teoretično napoved eksperimentalno preverimo tako, da eno izmed količin vzamemo za neodvisno spremenljivko, medtem ko ostale fiksiramo. Na sliki 3 so prikazane meritve kota odklona v odvisnosti od razdalje med kovinskima ploščama (slika 3a), mase krogle (slika 3b), potenciala na krogli (slika 3c) in napetosti med kovinskima ploščama (slika 3č). Vsako meritev (posamezna točka na grafih) smo opravili šestkrat, da smo povečali zanesljivost meritev. Vidimo, da se kot odmika res linearno povečuje, če se povečujeta napetost med ploščama in potencial krogle. Pri odvisnosti kota odmika od razdalje med ploščama in mase krogle pa opazimo, da se sicer kot manjša z večanjem razmika in mase, vendar obratne odvisnosti iz meritev ne moremo razbrati. Za meritve v območju razdalj med ploščama in mas kroglic, ki smo jih imeli na razpolago, se zdi odvisnost prej linearna kot obratno sorazmerna. Kljub temu pa so rezultati teh meritev dobro vodilo k najbolj optimalni izbiri parametrov pri drugi skupini meritev.



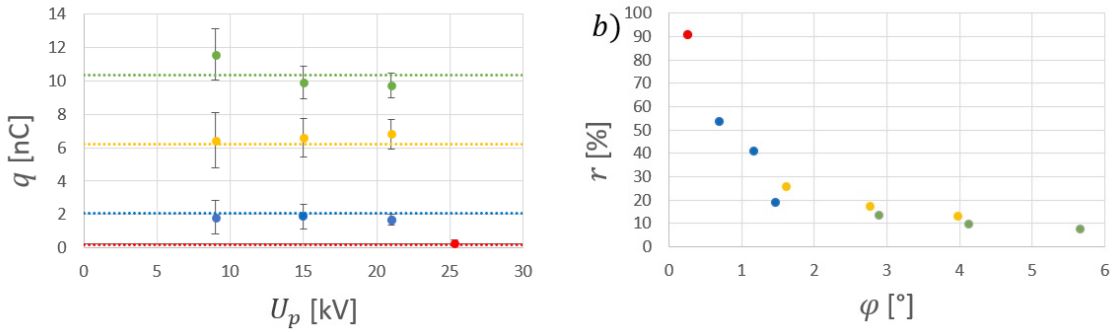
Slika 3. Odvisnost kota (φ), ki ga nitka v ravnovesni legi krogle oklepa z navpičnico, od a) razdalje (h) med kovinskima ploščama, b) mase (m) krogle, c) napetosti (U), s katero smo naelektrili krogle in č) napetosti med kovinskima ploščama (U_p). Meritve v primeru a) so bile izvedene z aluminijasto kroglo z maso 0,07 g, v b) z vsemi aluminijastimi kroglami, v primeru c) in č) pa z grafitno kroglo. Podatki o kroglah so zbrani v preglednici 1.

Naslednji sklop meritev smo izvedli samo z grafitno kroglo. Da bi ugotovili, kolikšen naboj na krogli lahko izmerimo z obravnavano metodo in kolikšna je napaka meritve, smo pri treh različnih potencialih krogle izmerili odklon nitke pri treh različnih napetostih med kovinskima ploščama. Za vsako kombinacijo potenciala krogle in napetosti med ploščama smo opravili po šest meritev. Pred vsako meritvijo smo kroglico razelektrili in ponovno naelektrili. Iz izmerjenega kota smo ob poznavanju ostalih parametrov izračunali naboj po enačbi (6), iz potenciala krogle pa še po enačbi (1). Meritve kotov in naboji, izračunani po obeh metodah, so zbrani v preglednici 2 in na sliki 4. Najmanjšo napako izmerjenega naboja in najmanjše odstopanje od naboja na krogli, ki ga izračunamo po enačbi (1), dosežemo pri meritvi, kjer je grafitna krogla s potencialom $U = 5{,}0\ \mathrm{kV}$ med ploščama, ki sta oddaljeni za $h = 15\ \mathrm{cm}$, napetost med njima pa je $U = 21{,}0\ \mathrm{kV}$. Za kot odklona smo izmerili $\varphi = 5{,}7° \pm 0{,}4°$. Ob

upoštevanju mase kroglice (glej preglednico 1), iz enačbe (6) izračunamo $q = 9{,}7(1 \pm 0{,}08)$ nC. Po enačbi (1) pa izračunamo $10{,}4(1 \pm 0{,}01)$ nC. Vrednosti se v okviru napake ujemata. Iz slike 4a vidimo, da se relativna napaka izmerjenega naboja manjša, če povečujemo U_p, vendar smo tu omejeni z dosegom generatorja. Če se manjša naboj na krogli, pa se napaka močno povečuje, kar je povezano z natančnostjo meritve kota odklona (slika 4b).
Meritev smo izvedli tudi z nabojem na krogli reda velikosti 0,1 nC. Kroglo smo naelektrili z napetostjo $U = 100$ V. Po enačbi (1) izračunamo, da smo nanjo nanesli naboj 0,24 nC. Napetost med ploščama smo nastavili na največjo možno, to je $U_p = 25{,}3$ kV, razdaljo med ploščama pa smo nastavili na $h = 10$ cm. Nitka se je odklonila za kot $\varphi = 0{,}3° \ (1 \pm 0{,}9)$. Vidimo, da je meritev popolnoma nezanesljiva, vendar z njo še vedno lahko določimo velikostni red naboja na krogli (glej Preglednico 2).

U_p [kV]	U [kV]	φ [°]	$q_{(1)}$ [nC]	$q_{(6)}$ [nC]
$9{,}00 \pm 0{,}01$	$1{,}00 \pm 0{,}01$	$0{,}7 \ (1 \pm 0{,}5)$	$2{,}07 \ (1 \pm 0{,}01)$	$2{,}8 \ (1 \pm 0{,}5)$
9,00	3,00	$1{,}6 \ (1 \pm 0{,}2)$	6,21	$6{,}4 \ (1 \pm 0{,}2)$
9,00	5,00	$2{,}9 \ (1 \pm 0{,}1)$	10,4	$11 \ (1 \pm 0{,}1)$
15,00	1,00	$1{,}2 \ (1 \pm 0{,}4)$	2,07	$2{,}9 \ (1 \pm 0{,}4)$
15,00	3,00	$2{,}2 \ (1 \pm 0{,}2)$	6,21	$5{,}3 \ (1 \pm 0{,}2)$
15,00	5,00	$4{,}1 \ (1 \pm 0{,}1)$	10,4	$9{,}8 \ (1 \pm 0{,}1)$
21,00	1,00	$1{,}5 \ (1 \pm 0{,}2)$	2,07	$2{,}6 \ (1 \pm 0{,}2)$
21,00	3,00	$3{,}0 \ (1 \pm 0{,}1)$	6,21	$5{,}1 \ (1 \pm 0{,}1)$
21,00	5,00	$5{,}7 \ (1 \pm 0{,}08)$	10,4	$9{,}8 \ (1 \pm 0{,}08)$
25,30	0,10	$0{,}3 \ (1 \pm 0{,}9)$	$0{,}2 \ (1 \pm 0{,}1)$	$0{,}3 \ (1 \pm 0{,}9)$

Preglednica 2: Podatki o izmerjenih nabojih; U_p je napetost med ploščama kondenzatorja, U potencial na plašču krogle, φ kot odklona nitke od navpičnice, $q_{(1)}$ naboj, izračunan po enačbi (1) in $q_{(6)}$ naboj, izračunan po enačbi (6).



Slika 4. a) Naboj (q) na krogli v odvisnosti od napetosti (U_p) med kovinskima ploščama in b) relativna napaka (r) izmerjenega odklona nitke (φ). Zelene točke: $U = 5{,}0$ kV, rumene točke: $U = 3{,}0$ kV, modre točke: $U = 1{,}5$ kV , rdeča točka: $U = 100$ V. Črtkane črte predstavljajo naboj, izračunan po enačbi (1).

5 ZAKLJUČEK

Predstavili smo preprost merilnik naboja, s katerim lahko izmerimo naboj na naelektreni prevodni krogli. Kroglo obesimo na tanko neprevodno nitko in jo postavimo med dve naelektreni kovinski plošči. Z merjenjem kota odklona nitke od navpičnice lahko določimo naboj na krogli. Izdelali smo več krogel iz alufolije, a je bila površina preveč hrapava, da bi lahko z njimi izvajali zanesljive meritve, so pa bile te krogle uporabne za preverjanje kvalitativne odvisnosti med kotom odklona nitke in maso krogle ter razdaljo med kovinskima ploščama. Meritve naboja smo izvedli z grafitno kroglo, ki je imela gladko površino, a tudi

večjo maso, zato so odkloni nitke bili manjši, glavna napaka meritve pa je prav v meritvi velikosti odklona. S pripomočki, ki smo jih imeli na razpolago, smo lahko izmerili naboj na krogli reda velikost 10 nC z 10 % natančnostjo, z manjšanjem naboja pa se napaka veča. Pri naboju reda velikosti 0,1 nC je meritev že popolnoma nezanesljiva. Če bi želeli izmeriti naboj manjši od 1 nC, bi potrebovali kroglo z manjšo maso in manjšim polmerom (glej enačbo (6)). Predstavljena metoda za merjenje majhnih nabojev ni uporabna za industrijske in gospodarske namene, lahko pa služi v študijskem procesu kot poučna alternativa coulombmetru.

Literatura

[1] Faletič, S. (2018). Kaj pa en YPT v razredu? Fizika v šoli, 23(1), 2 – 9; Pridobljeno: 28. 2. 2024.
[2] Problems for the 37th IYPT 2024, https://www.iypt.org/problems/problems-iypt-2024/ Pridobljeno: 28. 2. 2024.
[3] Franklin bells, https://en.wikipedia.org/wiki/Franklin_bells Pridobljeno: 28. 2. 2024.
[4] Saranin, V. A. (2014). About behaviour of electrostatic pendulum near conducting or dielectric plate. Journal of Electrostatics, 72(4), 235 – 241; Pridobljeno: 4. 3. 2024.
[5] ImageJ, Image Processing and Analysis in Java, https://imagej.net/ij/features.html Pridobljeno: 29. 2. 2024;

STROKOVNI PRISPEVKI

Dianoia 8 (2024) 79–89

Hosoyev polinom
The Hosoya polynomial

Nik Hrastnik

Univerza v Mariboru, Fakulteta za naravoslovje in matematiko, Koroška cesta 160, Maribor, Slovenija

Povzetek

V članku predstavimo Hosoyev polinom, ki se uporablja na področju kemijske teorije grafov. Opišemo Wienerjev indeks, ki je zelo znan in pomemben topološki indeks, ki ga definiramo s pomočjo razdalj med vozlišči v grafu, prav tako pa njegovo povezanost s Hosoyevim polinomom. Dokazano je namreč, da lahko omenjen indeks dobimo tako, da v prvi odvod Hosoyevega polinoma vstavimo vrednost 1. Predstavimo tudi poseben primer naslovnega polinoma, ki ga definiramo le za posamezna vozlišča grafa, in rekurzivno formulo za njegov izračun. Na koncu s pomočjo tega opišemo še splošno formulo za izračun Hosoyevega polinoma za linearne benzenoidne verige.

Ključne besede: Hosoyev polinom, Wienerjev indeks, linearna benzenoidna veriga

Abstract

In the article, we present the Hosoya polynomial, which is used in the field of chemical graph theory. We describe the Wiener index, which is a very well-known and important topological index defined using distances between vertices in a graph, as well as its connection to the Hosoya polynomial. It has been proven that this index can be obtained by substituting the value of 1 into the first derivative of the Hosoya polynomial. We also present a special case of the mentioned polynomial, defined only for individual vertices of the graph, and a recursive formula for its calculation. Finally, with the help of this, we describe a general formula for calculating the Hosoya polynomial for linear benzenoid chains.

Key words: the Hosoya polynomial, the Wiener index, linear benzenoid chains.

1 Uvod

Teorija grafov je področje matematike, ki proučuje strukturo in lastnosti grafov, ki so sestavljeni iz vozlišč in povezav med njimi. Uporabna je na številnih področjih, saj lahko grafe uporabimo kot modele različnih sistemov. Njihovo uporabo pogosto zasledimo v računalništvu, telekomunikacijah, prometu, ekonomiji, biologiji, kemiji in tudi drugih naravoslovnih in družboslovnih vedah. V tem članku bomo spoznali Hosoyev polinom in Wienerjev indeks, ki imata pomembno vlogo na področju kemije. Uporabita se lahko na primer za ugotavljanje temperature vrelišča za alkane. Več o tem najdemo v članku [3].

V naslednjem poglavju je podanih nekaj osnovnih pojmov iz teorije grafov, ki bodo potrebni v nadaljevanju članka. V poglavju 3 definiramo Hosoyev polinom in Wienerjev indeks ter zapišemo zvezo med njima. V poglavju 4 definiramo Hosoyev polinom za posamezna vozlišča grafa in zapišemo nekaj trditev iz članka [2], ki povezujejo te polinome z običajnim Hosoyevim polinomom grafa. V zadnjem poglavju definiramo še benzenoidne grafe, ki so matematični model za molekule, ki se v kemiji imenujejo benzenoidni

E-naslov: nik.hrastnik@student.um.si (Nik Hrastnik)

ogljikovodiki. Podrobneje si ogledamo rekurzivno formulo za izračun Hosoyevega polinoma linearnih benzenoidnih verig, ki jo dobimo kot posledico rezultatov iz poglavja 4, zaključimo pa z izpeljavo splošne formule za izračun Hosoyevega polinoma takih verig.

2 Osnovni pojmi teorije grafov

Kot že omenjeno, bomo v tem poglavju predstavili nekaj osnovnih definicij iz teorije grafov, ki bodo potrebne za nadaljnje razumevanje obravnavanih tem. Bolj podrobne informacije lahko najdemo v [4].

Najbolj osnovni pojem v teoriji grafov je graf G, ki ga definiramo kot urejen par neprazne množice vozlišč $V(G)$ in množice neurejenih parov vozlišč $E(G)$, ki jim rečemo povezave, torej $G = (V(G), E(G))$. Vozlišča običajno rišemo kot točke, povezave pa kot črte med njimi. Povezavo označimo kot $e = uv$, kjer sta $u, v \in V(G)$. V tem primeru pravimo, da sta u in v sosednji vozlišči ter da sta krajišči povezave e.

Pot v grafu od vozlišča v_1 do vozlišča v_n je zaporedje povezav $v_1v_2, v_2v_3, \ldots, v_{n-1}v_n$, kjer so $v_1, v_2, \ldots v_n$ paroma različna vozlišča.

Cikel v grafu je zaporedje povezav $v_1v_2, v_2v_3, \ldots, v_{n-1}v_n, v_nv_1$, kjer so $v_1, v_2, \ldots v_n$ paroma različna vozlišča. Cikel, v katerem je vključenih n vozlišč, imenujemo n-cikel.

Graf G je povezan, če za poljubni vozlišči u in v obstaja pot od u do v, sicer je graf nepovezan. V povezanem grafu G lahko za poljubni vozlišči definiramo razdaljo med njima. Dolžina poti od u do v je enaka številu povezav na tej poti, razdalja od u do v pa je definirana kot dolžina najkrajše poti v grafu G od u do v. Razdaljo od u do v označujemo kot $d(u, v)$.

3 Hosoyev polinom in Wienerjev indeks

Leta 1988 je Hosoya [1] vpeljal polinom, ki ga je označil kot $H(G, x)$ in ga definiral na naslednji način: Naj bo G povezan graf z n vozlišči in m povezavami. Če $d(G, k)$ označuje število neurejenih parov vozlišč v grafu G na razdalji k, potem

$$H(G) = H(G, x) = \sum_{k \geq 0} d(G, k)x^k \tag{3.1}$$

imenujemo Hosoyev polinom grafa G. Opozorimo na to, da je $d(G, 0) = n$ in $d(G, 1) = m$.

Opomnimo, da je Hosoya ta polinom ob vpeljavi imenoval Wienerjev polinom. Glavni razlog za to je pomembna zveza med Hosoyevim polinomom in Wienerjevim indeksom, ki bo podana v nadaljevanju, se je pa pozneje vseeno bolj uveljavilo ime Hosoyev polinom.

Da pa bomo lahko razložili omenjeno zvezo, najprej definirajmo Wienerjev indeks. Vpeljal ga je ameriški kemik Harold Wiener leta 1947. Za tem je odkril še veliko povezav med omenjenim indeksom in kemijskimi lastnostmi alkanov, ki so pomembne spojine v kemiji. Več o tem je mogoče prebrati v [3]. Wienerjev indeks ali Wienerjevo število grafa G definiramo kot vsoto dolžin najkrajših poti med vsemi pari vozlišč v grafu G:

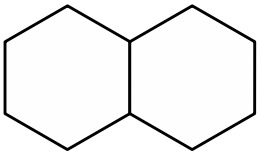
$$W = W(G) = \sum_{\{x,y\} \subseteq V(G)} d(x, y). \tag{3.2}$$

Neposredno iz definicij sledi že večkrat omenjena zveza med Hosoyevim polinomom in Wienerjevim indeksom:

$$H'(G,1) = W(G), \tag{3.3}$$

pri čemer je $H'(G,1)$ prvi odvod Hosoyevega polinoma, izračunan v točki $x = 1$.

Teorija grafov je tudi nasploh uporabna v kemiji, saj za dano molekulo z lahkoto tvorimo graf tako, da za vozlišča grafa vzamemo atome molekule, za povezave pa kemijske vezi med atomi. Vodikove atome običajno zanemarimo. Oglejmo si primer, kjer na opisan način predstavimo graf benzenoidnega ogljikovodika naftalena. Za podan graf bomo zapisali Hosoyev polinom in nato še Wienerjev indeks s pomočjo zgornje formule.



G

Slika 1: Graf benzenoidnega ogljikovodika naftalena.

Naj bo G graf, ki je podan na sliki 1. Upoštevamo definicijo (3.1) in tako za graf G dobimo pripadajoči Hosoyev polinom: $H(G,x) = 10+11x+14x^2+12x^3+6x^4+2x^5$. Da bomo lahko izračunali Wienerjev indeks, zapišimo še prvi odvod polinoma: $H'(G,x) = 11 + 28x + 36x^2 + 24x^3 + 10x^4$. V odvod vstavimo $x = 1$ in dobimo iskani indeks: $W(G) = H'(G,1) = 11 + 28 + 36 + 24 + 10 = 109$.

Opomnimo, da bomo benzenoidne ogljikovodike natančneje definirali v poglavju o linearnih benzenoidnih verigah, kjer bomo izpeljali tudi splošno formulo za izračun Hosoyevega polinoma takih verig. V to skupino sodi tudi ravnokar obravnavani naftalen, zato bomo lahko preverili pravilnost izračuna njegovega Hosoyevega polinoma.

4 Rekurzivna formula za izračun Hosoyevega polinoma

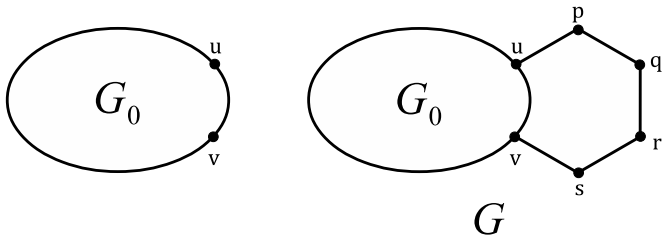
V tem poglavju nas bodo zanimali grafi, ki jih lahko konstruiramo tako, da na neko povezavo manjšega grafa dodamo 6-cikel. Za take grafe bomo zapisali rekurzivno formulo za izračun Hosoyevega polinoma s pomočjo Hosoyevega polinoma manjšega grafa, kar je bilo prvič predstavljeno v članku [2]. V tej formuli se pojavi tudi Hosoyev polinom za neko vozlišče grafa, zato najprej dodajmo še to definicijo.

Naj bo G poljuben povezan graf, $v \in V(G)$ poljubno vozlišče in $k \geq 0$. Naj bo še $d(G,v,k)$ število vseh vozlišč grafa G, ki so od vozlišča v oddaljena za k. Velja, da je $d(G,v,0) = 1$, dodatno pa še definiramo $d(G,v,k) = 0$ za vse $k < 0$. Potem definiramo $H(G,v,x)$ na naslednji način:

$$H(G,v,x) = \sum_{k\geq 0} d(G,v,k)x^k.$$

Trditev 4.1. *[2] Naj bo G graf, dobljen iz grafa G_0 z dodajanjem 6-cikla na povezavo uv (glej sliko 2). Potem velja:*

$$\begin{aligned} H(G,x) =& H(G_0,x) + xH(G_0,u,x) + x^2H(G_0,u,x) + xH(G_0,v,x) + x^2H(G_0,v,x) \\ &+ 4 + 3x + 2x^2 + x^3. \end{aligned}$$



Slika 2: Graf G, ki ga dobimo z dodajanjem 6-cikla grafu G_0 na povezavo uv.

Dokaz. Najprej zapišemo Hosoyev polinom v naslednji obliki:

$$H(G,x) = d(G,0) + d(G,1)x + d(G,2)x^2 + d(G,3)x^3 + \sum_{k\geq 4} d(G,k)x^k. \qquad (4.1)$$

Naj $d(G_0,k,u,v)$ označuje naslednji izraz:

$$d(G_0,k) + d(G_0,u,k-1) + d(G_0,u,k-2) + d(G_0,v,k-1) + d(G_0,v,k-2). \quad (4.2)$$

Ugotovimo, da velja:

$$d(G,k) = \begin{cases} d(G_0,k,u,v); & k > 3, \\ d(G_0,k,u,v)+1; & k = 3, \\ d(G_0,k,u,v)+2; & k = 2, \\ d(G_0,k,u,v)+3; & k = 1, \\ d(G_0,k,u,v)+4; & k = 0. \end{cases} \qquad (4.3)$$

Namreč, prvi člen izraza (4.2) označuje število parov vseh vozlišč, ki so v grafu G_0 na razdalji k. Da bomo dobili število parov vseh vozlišč na razdalji k v grafu G, moramo temu prišteti še $d(G_0,u,k-1)$ in $d(G_0,u,k-2)$, saj je na novo dodano vozlišče p na razdalji k z vsemi tistimi vozlišči, s katerimi je bil u na razdalji $k-1$. Podobno je q na razdalji k z vsemi tistimi vozlišči, s katerimi je bil u na razdalji $k-2$. Podobno lahko razložimo, zakaj sta v tem izrazu prišteti še števili $d(G_0,v,k-1)$ in $d(G_0,v,k-2)$. V primeru $k=0$ prištejemo 4, saj smo na novo dobili 4 vozlišča, pri $k=1$ pa smo prišteli 3 pare, in sicer $\{p,q\},\{q,r\},\{r,s\}$. Opomnimo, da sta para $\{u,p\}$ in $\{s,v\}$ šteta že pri $d(G_0,k,u,v)$. Podobno smo pri $k=2$ prišteli para $\{p,r\}$ in $\{q,s\}$ ter par $\{p,s\}$ pri $k=3$.

Če (4.3) vstavimo v (4.1), ugotovimo, da lahko Hosoyev polinom grafa G izrazimo na naslednji način:

$$\sum_{k\geq 0} d(G_0,k,u,v)x^k + 4 + 3x + 2x^2 + x^3,$$

kar pa je enako

$$H(G_0,x) + xH(G_0,u,x) + x^2H(G_0,u,x) + xH(G_0,v,x) + x^2H(G_0,v,x) + 4 + 3x + 2x^2 + x^3.$$

□

V naslednjem poglavju bomo s pomočjo dokazane trditve izpeljali splošno formulo za izračun Hosoyevega polinoma linearnih benzenoidnih verig. Za to bomo potrebovali še rekurzivno formulo za izračun $H(G,q,x)$ in $H(G,r,x)$, pri čemer so G,q in r kot na sliki 2. Kako to storimo, nam pove naslednja trditev.

Trditev 4.2. *[2] Naj bodo G, G_0, q in r taki, kot so prikazani na sliki 2. Potem velja:*

(i) $H(G,q,x) = x^2 H(G_0,u,x) + 1 + 2x + x^2$,

(ii) $H(G,r,x) = x^2 H(G_0,v,x) + 1 + 2x + x^2$.

Dokaz. Zaradi simetrije vozlišč q in r zadošča dokazati samo točko (i). Najprej opazimo, da velja

$$d(G,q,k) = \begin{cases} d(G_0,u,k-2); & k > 2, \\ d(G_0,u,k-2)+1; & k = 2, \\ d(G_0,u,k-2)+2; & k = 1, \\ d(G_0,u,k-2)+1; & k = 0, \end{cases}$$

kar razložimo na podoben način, kot smo to naredili za formulo (4.3) v dokazu prejšnje trditve. Iz tega potem sledi:

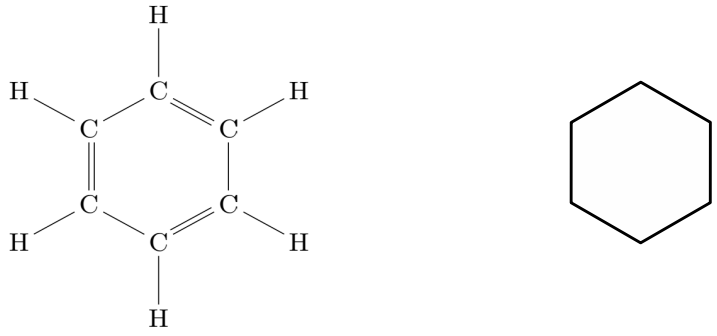
$$\begin{aligned} H(G,q,x) &= \sum_{k\geq 0} d(G,q,k)x^k = \sum_{k\geq 0} d(G_0,u,k-2)x^k + 1 + 2x + x^2 \\ &= x^2 H(G_0,u,x) + 1 + 2x + x^2. \end{aligned}$$

□

5 Linearne benzenoidne verige

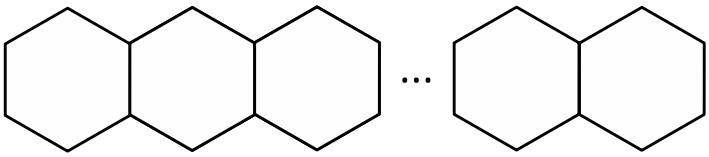
Sedaj bomo izračunane rekurzivne formule uporabili za izračun splošne formule Hosoyevega polinoma linearnih benzenoidnih verig. Omenimo, da so bile takšne formule za poljubne benzenoidne verige obravnavane v članku [2].

Benzenoidni ogljikovodiki so aromatski ogljikovodiki, ki so sestavljeni iz samih benzenovih obročev. Benzen je kemična spojina s formulo C_6H_6, ki vsebuje proste π-elektrone. Njihovo razporeditev velikokrat ponazorimo s Kekulejevimi strukturami, kjer uporabimo dvojne vezi. Opozorimo na to, da bomo zaradi enostavnosti na slikah grafov izpuščali vodikove atome in dvojne vezi, torej bomo graf benzena predstavili kar kot 6-cikel.



Slika 3: (a) Molekula benzena in (b) njen benzenoidni graf.

O linearnih benzenoidnih verigah govorimo, ko je skupaj združenih več benzenovih obročev tako, kot prikazuje slika 4. Primer take verige z dvema benzenovima obročema

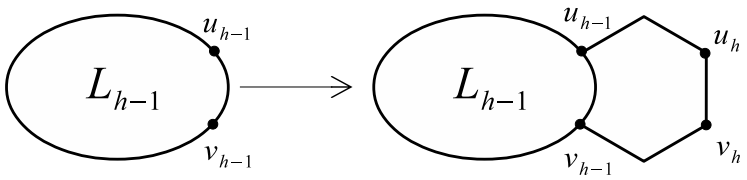


Slika 4: Linearna benzenoidna veriga.

smo že obravnavali v poglavju o Hosoyevem polinomu in Wienerjevem indeksu in je viden na sliki 1, na sliki 4 pa lahko vidimo še splošno linearno benzenoidno verigo.

Za $h \geq 1$ naj sedaj L_h označuje linearno benzenoidno verigo s h benzenovimi obroči, ki smo jo dobili z dodajanjem 6-cikla grafu L_{h-1} na povezavo $u_{h-1}v_{h-1}$, kot je označena na sliki 5. Opomnimo, da je L_0 graf, ki ga sestavlja samo ena povezava u_0v_0. Po trditvi 4.1 potem sledi:

$$\begin{aligned} H(L_h, x) =& H(L_{h-1}, x) + (x + x^2)(H(L_{h-1}, u_{h-1}, x) + H(L_{h-1}, v_{h-1}, x)) \\ &+ 4 + 3x + 2x^2 + x^3. \end{aligned} \tag{5.1}$$



Slika 5: Konstrukcija linearne benzenoidne verige.

Naj bo še u_hv_h tista povezava grafa L_h, na katero bomo napeli naslednji 6-cikel, če bomo želeli nadaljevati našo verigo, torej iz L_h dobiti L_{h+1}. Za izbiro te povezave imamo v splošnem več možnosti, mi pa povezavo izberemo tako, da ohranimo linearnost verige. O ostalih možnostih in rezultatih, ki so povezani s tem, lahko več izvemo v [2]. Še enkrat opozorimo, da obravnavamo le primer linearne verige, torej tisto izbiro povezave u_hv_h, ki je prikazana na sliki 5. Z uporabo trditve 4.2 ugotovimo naslednje:

$$\begin{aligned} H(L_h, u_h, x) &= x^2 H(L_{h-1}, u_{h-1}, x) + 1 + 2x + x^2, \\ H(L_h, v_h, x) &= x^2 H(L_{h-1}, v_{h-1}, x) + 1 + 2x + x^2. \end{aligned} \tag{5.2}$$

Za lažji zapis do sedaj zapisanih formul vpeljimo naslednje oznake: $\alpha_h := H(L_h, x)$, $\beta_h := H(L_h, u_h, x)$ in $\gamma_h := H(L_h, v_h, x)$. Potem sledi naslednja trditev:

Trditev 5.1. *[2] Naj bo L_h linearna benzenoidna veriga s h benzenovimi obroči. Potem za vsak $h \geq 1$ veljajo naslednje rekurzivne zveze:*

(i) $\alpha_h = \alpha_{h-1} + (x + x^2)(\beta_{h-1} + \gamma_{h-1}) + 4 + 3x + 2x^2 + x^3$,

(ii) $\beta_h = x^2\beta_{h-1} + 1 + 2x + x^2$,

(iii) $\gamma_h = x^2\gamma_{h-1} + 1 + 2x + x^2$,

pri čemer je $\alpha_0 = 2 + x$ *in* $\beta_0 = \gamma_0 = 1 + x$.

Dokaz. Rekurzivne zveze sledijo neposredno iz formul (5.1) in (5.2). Zlahka preverimo, da je $\alpha_0 = H(L_0, x) = 2 + x$, $\beta_0 = H(L_0, u_0, x) = 1 + x$ in $\gamma_0 = H(L_0, v_0, x) = 1 + x$. □

Opomba. *Ker je $\beta_0 = \gamma_0$, posledično velja tudi $\beta_h = \gamma_h$, za vsak $h > 0$. To sledi iz dejstva, da u_h in v_h v grafu nastopata simetrično.*

Sedaj bomo s pomočjo zapisanih rekurzivnih zvez izpeljali splošno formulo za izračun β_h in γ_h, s pomočjo tega pa še splošno formulo za izračun α_h.

Trditev 5.2. *Za vsak $h \geq 0$ velja:*

$$\beta_h = \gamma_h = \frac{(x^2 + x)x^{2h} - x - 1}{x - 1}.$$

Dokaz. Trditev bomo dokazali z indukcijo, in sicer le za β_h, saj sta vrednosti β_h in γ_h enaki. Najprej preverimo, če zapisana zveza velja za $h = 0$:

$$\beta_0 = \frac{(x^2 + x)x^0 - x - 1}{x - 1} = \frac{x^2 + x - x - 1}{x - 1}$$

$$= \frac{x^2 - 1}{x - 1} = \frac{(x - 1)(x + 1)}{x - 1} = x + 1.$$

Po trditvi 5.1 vemo, da to velja. Preverimo še za $h = 1$:

$$\beta_1 = \frac{(x^2 + x)x^2 - x - 1}{x - 1} = \frac{(x + 1)x^3 - x - 1}{x - 1}$$

$$= \frac{(x + 1)x^3 - (x + 1)}{x - 1} = \frac{(x + 1)(x^3 - 1)}{x - 1}$$

$$= \frac{(x + 1)(x - 1)(x^2 + x + 1)}{x - 1} = (x + 1)(x^2 + x + 1)$$

$$= x^3 + x^2 + x + x^2 + x + 1 = x^3 + 2x^2 + 2x + 1.$$

Tudi ta izračun je ustrezen, saj za poljubno vozlišče grafa L_1, ki vsebuje samo en benzenov obroč, velja, da je eno vozlišče od njega oddaljeno za 3, dve vozlišči za 2 in dve vozlišči za 1.
Naj bo $h > 1$ poljuben. Predpostavimo, da formula velja za $h - 1$, torej da je

$$\beta_{h-1} = \frac{(x^2 + x)x^{2h-2} - x - 1}{x - 1},$$

dokazujemo pa, da velja za h. Uporabili bomo že izpeljano rekurzivno formulo iz trditve 5.1:

$$\begin{aligned}
\beta_h &= x^2\beta_{h-1} + 1 + 2x + x^2 \\
&= x^2\frac{(x^2+x)x^{2h-2} - x - 1}{x-1} + 1 + 2x + x^2 \\
&= \frac{(x^2+x)x^{2h} - x^3 - x^2}{x-1} + 1 + 2x + x^2 \\
&= \frac{(x^2+x)x^{2h} - x^3 - x^2 + (x-1) + 2x(x-1) + x^2(x-1)}{x-1} \\
&= \frac{(x^2+x)x^{2h} - x^3 - x^2 + x - 1 + 2x^2 - 2x + x^3 - x^2}{x-1} \\
&= \frac{(x^2+x)x^{2h} - x - 1}{x-1}.
\end{aligned}$$

□

S pomočjo računalniških programov za simbolno računanje lahko rešimo rekurzijo za α_h iz trditve 5.1, od koder dobimo idejo za naslednji rezultat.

Izrek 5.3. *[2] Za vsak $h \geq 0$ velja:*

$$\alpha_h = \frac{2(x+1)x^{2h+2} - x^3 - 2x^2 - 3x + h(x-1)(x^2+1)(x^2-x-4) + 2}{(x-1)^2}.$$

Dokaz. Tudi tokrat bomo uporabili indukcijo. Preverimo najprej za $h = 0$:

$$\begin{aligned}
\alpha_0 &= \frac{2(x+1)x^2 - x^3 - 2x^2 - 3x + 2}{(x-1)^2} \\
&= \frac{2x^3 + 2x^2 - x^3 - 2x^2 - 3x + 2}{(x-1)^2} \\
&= \frac{x^3 - 3x + 2}{(x-1)^2} = \frac{(x+2)(x-1)^2}{(x-1)^2} = x + 2,
\end{aligned}$$

to pa velja po trditvi 5.1. Naj bo sedaj $h > 0$ poljuben. Predpostavimo, da formula velja za $h-1$, torej da je

$$\alpha_{h-1} = \frac{2(x+1)x^{2(h-1)+2} - x^3 - 2x^2 - 3x + (h-1)(x-1)(x^2+1)(x^2-x-4) + 2}{(x-1)^2},$$

dokazujemo pa, da velja za h. α_h najprej zapišemo s pomočjo rekurzivne zveze iz trditve 5.1, v drugem koraku pa uporabimo indukcijsko predpostavko in formuli za β_{h-1} in γ_{h-1} iz trditve 5.2.

$$\alpha_h = \alpha_{h-1} + (x + x^2)(\beta_{h-1} + \gamma_{h-1}) + 4 + 3x + 2x^2 + x^3$$

$$= \frac{2(x+1)x^{2(h-1)+2} - x^3 - 2x^2 - 3x + (h-1)(x-1)(x^2+1)(x^2-x-4) + 2}{(x-1)^2}$$

$$+ (x+x^2)\left(2\frac{(x^2+x)x^{2h-2} - x - 1}{x-1}\right) + 4 + 3x + 2x^2 + x^3$$

$$= \frac{2(x+1)x^{2h} - x^3 - 2x^2 - 3x + h(x-1)(x^2+1)(x^2-x-4)}{(x-1)^2}$$

$$+ \frac{-(x-1)(x^2+1)(x^2-x-4) + 2}{(x-1)^2} + (x+x^2)\frac{2x^{2h} + 2x^{2h-1} - 2x - 2}{x-1}$$

$$+ 4 + 3x + 2x^2 + x^3$$

$$= \frac{2x^{2h+1} + 2x^{2h} - x^3 - 2x^2 - 3x + h(x-1)(x^2+1)(x^2-x-4)}{(x-1)^2}$$

$$+ \frac{-x^5 + 2x^4 + 2x^3 - 2x^2 + 3x - 4 + 2}{(x-1)^2}$$

$$+ \frac{(4 + 3x + 2x^2 + x^3)(x^2 - 2x + 1)}{(x-1)^2}$$

$$+ \frac{2x^{2h+1} + 2x^{2h} - 2x^2 - 2x + 2x^{2h+2} + 2x^{2h+1} - 2x^3 - 2x^2}{x-1}$$

$$= \frac{2x^{2h+1} + 2x^{2h} - x^3 - 2x^2 - 3x + h(x-1)(x^2+1)(x^2-x-4)}{(x-1)^2}$$

$$+ \frac{-x^5 + 2x^4 + 2x^3 - 2x^2 + 3x - 4 + 2 + x^5 - 5x + 4}{(x-1)^2}$$

$$+ \frac{2x^{2h+2} + 4x^{2h+1} + 2x^{2h} - 2x^3 - 4x^2 - 2x}{x-1}$$

$$= \frac{2x^{2h+1} + 2x^{2h} - x^3 - 2x^2 - 3x + h(x-1)(x^2+1)(x^2-x-4)}{(x-1)^2}$$

$$+ \frac{2x^4 + 2x^3 - 2x^2 - 2x + 2}{(x-1)^2}$$

$$+\frac{2x^{2h+3}+4x^{2h+2}+2x^{2h+1}-2x^4-4x^3-2x^2}{(x-1)^2}$$

$$+\frac{-2x^{2h+2}-4x^{2h+1}-2x^{2h}+2x^3+4x^2+2x}{(x-1)^2}$$

$$=\frac{2x^{2h+1}+2x^{2h}-x^3-2x^2-3x+h(x-1)(x^2+1)(x^2-x-4)}{(x-1)^2}$$

$$+\frac{2x^4+2x^3-2x^2-2x+2}{(x-1)^2}$$

$$+\frac{2x^{2h+3}+2x^{2h+2}-2x^{2h+1}-2x^{2h}-2x^4-2x^3+2x^2+2x}{(x-1)^2}$$

$$=\frac{-x^3-2x^2-3x+h(x-1)(x^2+1)(x^2-x-4)+2+2x^{2h+3}+2x^{2h+2}}{(x-1)^2}$$

$$=\frac{2(x+1)x^{2h+2}-x^3-2x^2-3x+h(x-1)(x^2+1)(x^2-x-4)+2}{(x-1)^2}.$$

□

Posledica 5.4. *Za vsak $h \geq 0$ za Wienerjev indeks grafa L_h velja:*

$$W(L_h)=\frac{1}{3}(16h^3+36h^2+26h+3).$$

Dokaz. Če odvajamo enakost (5.1), uporabimo trditev 5.2 in opazujemo limito dobljene enakosti, ko gre x proti 1, dobimo naslednjo rekurzivno zvezo:

$$W(L_h)=W(L_{h-1})+16h^2+40h+26.$$

Če upoštevamo, da je $W(L_0)=1$, s pomočjo indukcije ni težko preveriti, da zares velja formula, ki smo jo želeli dokazati. □

Opomba. *Formulo za Wienerjev indeks grafa L_h so obravnavali že na primer v člankih [2], [5] in [6].*

Za konec oba rezultata uporabimo še na primeru benzenoidnega ogljikovodika naftalena, ki smo ga že obravnavali v tretjem poglavju, ko smo izračunali njegov Hosoyev polinom in Wienerjev indeks. Pravilnost rezultatov lahko sedaj preverimo z na novo izpeljanima formulama. Ker je naftalen sestavljen iz dveh benzenovih obročev (njegov graf je viden na sliki 1), bomo v omenjeni formuli vstavili vrednost $h=2$:

$$\alpha_2=\frac{2(x+1)x^{4+2}-x^3-2x^2-3x+2(x-1)(x^2+1)(x^2-x-4)+2}{(x-1)^2}$$

$$= \frac{2(x+1)x^6 - x^3 - 2x^2 - 3x + 2(x^5 - 2x^4 - 2x^3 + 2x^2 - 3x + 4) + 2}{(x-1)^2}$$

$$= \frac{2x^7 + 2x^6 - x^3 - 2x^2 - 3x + 2x^5 - 4x^4 - 4x^3 + 4x^2 - 6x + 8 + 2}{(x-1)^2}$$

$$= \frac{2x^7 + 2x^6 + 2x^5 - 4x^4 - 5x^3 + 2x^2 - 9x + 10}{(x-1)^2}$$

$$= \frac{(10 + 11x + 14x^2 + 12x^3 + 6x^4 + 2x^5)(x-1)^2}{(x-1)^2}$$

$$= 10 + 11x + 14x^2 + 12x^3 + 6x^4 + 2x^5.$$

Vidimo, da smo za Hosoyev polinom dobili enak rezultat. Podobno ugotovimo tudi, ko poračunamo še Wienerjev indeks:

$$W(L_2) = \frac{1}{3}(16 \cdot 2^3 + 36 \cdot 2^2 + 26 \cdot 2 + 3)$$

$$= \frac{1}{3}(16 \cdot 8 + 36 \cdot 4 + 52 + 3)$$

$$= \frac{327}{3} = 109.$$

Literatura

[1] H. Hosoya, On some counting polynomials in chemistry, *Discrete Appl. Math.* **19** (1988), 239–257.

[2] I. Gutman, S. Klavžar, M. Petkovšek, P. Žigert, On Hosoya polynomials of benzenoid graphs, *MATCH Commun. Math. Comput. Chem.* **43** (2001), 49–66.

[3] I. Gutman, Y.-N. Yeh, S.-L. Lee, Y.-L. Luo, Some recent results in the theory of Wiener number, *Indian J. Chem.* **32A** (1993), 651-661.

[4] R. J. Wilson, J. J. Watkins (prevod: Janez Žerovnik), *Uvod v teorijo grafov*, DMFA, Ljubljana, 1997.

[5] I. Gutman, O. E. Polansky, Wiener numbers of polyacenes and related benzenoid molecules, *MATCH Commun. Math. Comput. Chem.* **20** (1986), 115–123.

[6] D. Bonchev, Ov. Mekenyan, N. Trinajstić, Topological characterization of cyclic structures, *Int. J. Quantum Chem.* **17** (1980), 845–893.

Dianoia 8 (2024) 91-100

Reakcija litija s steklom

The lithium reaction with glass

Brina Dojer, Domen Ornik

Fakulteta za naravoslovje in matematiko, Koroška cesta 160, 2000 Maribor

Povzetek

V prispevku poročava o reakciji kovine I. skupine periodnega sistema, in sicer litija, s steklom. Ob opravljanju poskusov z natrijem, prav tako elementom prve skupine periodnega sistema, in pregledu literature sva naletela na zanimiv posnetek reakcije litija s steklom. Litij izkorišča kisik iz silicijevega dioksida, SiO_2, ki je glavna sestavina stekla, in zreagira v litijev oksid, Li_2O. Opravila sva poskuse, pri katerih sva dala litij v epruvete različnih proizvajalcev in z različno sestavo stekla ter opazovala reakcije. Litij je ob segrevanju v epruvetah s steklom reagiral, kar je jasno vidno s fotografij, ki jih prilagava v nadaljevanju.

Ključne besede: litij, steklo, periodni sistem, epruvete, kemijska reakcija

Abstract

In this paper, we report on the reaction of a metal of the first group of the periodic table, lithium, with glass. While conducting experiments with sodium, also an element of the first group of the periodic table, and reviewing the literature, we came across an interesting recording of the reaction of lithium with glass. Lithium utilizes oxygen from silicon dioxide, SiO_2, which is the main component of glass, and reacts to form lithium oxide, Li_2O. We performed experiments in which we placed lithium in test tubes of different manufacturers and with different glass compositions and observed the reactions. Lithium reacted when heated in test tubes with glass, which is clearly visible from the photos attached below.

Key words: lithium, glass, periodic table, test tubes, chemical reaction

1 UVOD

Litij je kemijski element v prvi skupini periodnega sistema (PS), ki jo imenujemo alkalijske kovine. Ta mehka srebrnobela kovina z gostoto 0,534 g/cm^3 je najlažja znana kovina. Je zelo reaktiven, na zraku takoj reagira z dušikom, nastane litijev nitrid, Li_3N, in postane temne barve. Če ga takrat povonjamo, ima vonj po amonijaku, NH_3, saj na zraku plast litijevega nitrida reagira z zračno vlago:

$$6Li + 3N_2 \rightarrow 2Li_3N$$

$$2Li_3N + 6H_2O \rightarrow 6LiOH + 2NH_3$$

Če ga damo v vodo, zreagira v litijev hidroksid, nastaja pa tudi vodik:

$$2Li + 2H_2O \rightarrow 2LiOH + H_2$$

V literaturi najdemo podatek, da ga, podobno kot natrij in kalij iz iste skupine PS, shranjujemo v petroleju [1].

Za razliko od ostalih alkalijskih kovin se nahaja v kamninah, od koder izvira tudi njegovo ime (gr. *lithos* = kamen).

Njegovo tališče je najvišje glede na ostale alkalijske kovine, in sicer 180,54 °C. Ob segrevanju v steklovini se stali, zažari in reagira s steklom. Kljub temu da je steklo inertno, litij izkorišča

E-mail naslov/i: brina.dojer@um.si (Brina Dojer), domen.ornik@student.um.si (Domen Ornik)

kisik iz silicijevega dioksida, SiO_2, ki je glavna sestavina stekla, in zreagira v litijev oksid, Li_2O (bela snov).

Črna snov, ki ostane v epruveti, je silicij, Si. Reakcija, ki poteče [2]:

$$4Li + SiO_2 \rightarrow 2Li_2O + Si$$

Steklo epruvete poči [3,4]. S steklom reagirata tudi fluorovodikova kislina, HF(aq) in koncentrirana raztopina natrijevega hidroksida, NaOH(aq), vendar nobena od reakcij ni burna.

Zelo zanimivo je, da natrij, ki je reaktivnejši od litija, s steklom ne reagira pri segrevanju v epruveti. Njegovo tališče je nižje kot litijevo, in sicer 97,79 °C. Razlog lahko iščemo v majhnosti litijevega atoma. Zato tudi spontano reagira z dušikom, ki velja za inertnega.

Laboratorijska stekla imajo ime in oznako, ki ju najdemo na samem izdelku ali na škatli, v kateri smo ga prejeli. Ločimo več vrst stekel za laboratorijsko steklovino. Razlikujejo se po vsebnosti spojin, ki jih vsebujejo. Navedenih je nekaj:

Natrijevo steklo (soda lime glass): sestavljeno je iz 60–75 % SiO_2, 12–18 % Na_2O in 5–12 % CaO [5]. Dodatek Na_2O in CaO zniža tališče na ≈ 750 ºC. Kot surovini v procesu proizvodnje stekla se uporabljata Na_2CO_3 in $CaCO_3$, soda in apnenec, ki med segrevanjem razpadeta na oksida:

$$Na_2CO_3 \rightarrow Na_2O + CO_2$$

$$CaCO_3 \rightarrow CaO + CO_2$$

Odpornost proti jedkim kemikalijam ni preveč dobra. Poznano je tudi kot ceneno steklo za okenske šipe, steklenice ipd.

Borosilikatno steklo ali bor-silicijevo steklo (Pyrex, Boral, Duran): del SiO_2 je zamenjan z borovim oksidom, B_2O_3, in vsebuje 70–80 % kremenčevega peska (SiO_2), 7–13 % borovega oksida (B_2O_3) in 5–10 % sode, (Na_2CO_3). Dodatek B_2O_3, predvsem pa nizek odstotek natrijevih, kalijevih in kalcijevih spojin poveča toplotno in kemijsko odpornost stekla: razteznostni koeficient 3×10^{-6}/ ºC. Uporabljajo ga za kemijsko steklovino in kuhinjsko posodje. Zelo odporno je proti kemikalijam in temperaturnim spremembam ter mehanskim obremenitvam.

Aluminij-silicijevo steklo vsebuje namesto B_2O_3 aluminijev oksid, Al_2O_3, ima dobro kemijsko in temperaturno odpornost.

Kalijevo-kalcijevo steklo: vsebuje kremenčev pesek (SiO_2), apnenec ($CaCO_3$) in pepeliko (K_2CO_3). Slednja v procesu taljenja razpade na K_2O:

$$K_2CO_3 \rightarrow K_2O + CO_2$$

Ta vrsta stekla se zmehča pri cca. 700 °C, zato ga uporabljajo za epruvete, kot "češko kristalno steklo" in "kronsko steklo" za optične naprave.

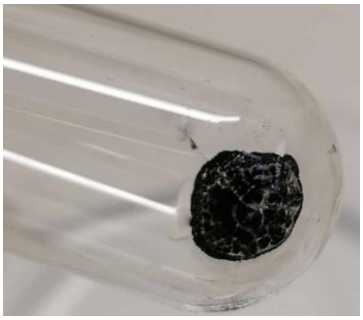
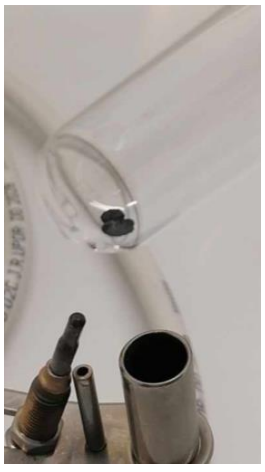
Silicijevo steklo ali kvarčno steklo vsebuje samo silicijev dioksid in velja za najdražje steklo. Ima visoko temperaturno odpornost (krajši čas je lahko izpostavljeno temperaturam do 1200 °C, medtem ko je njegova $T_{tališča} \approx 1600$ °C) [5].

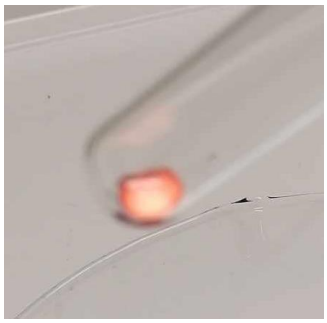
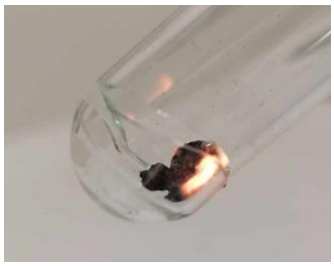
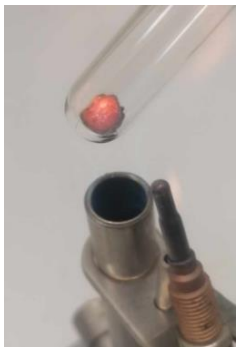
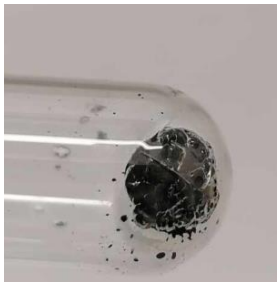
2 EKSPERIMENTALNO DELO

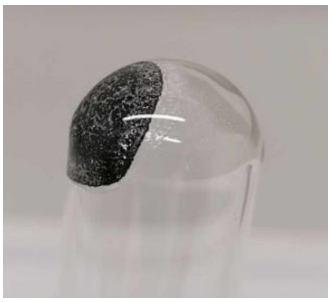
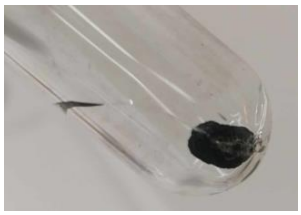
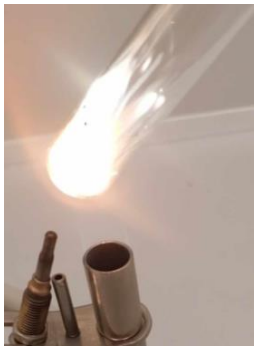
Pri delu sva uporabila epruvete različnih proizvajalcev in različnih kvalitet. V vsako od teh sva dala po cca. 2 koščka elementarnega litija, katerih masa je bila med 0,017 in 0,020 g. Ob segrevanju epruvete nad plinskim gorilnikom sva uporabila svetleči plamen, katerega temperatura je bila okoli 500 °C. Litij je po krajšem segrevanju zažarel, zagorel, epruveta pa je zaradi reakcije in visoke temperature počila. V nekaterih primerih je v epruveti ostala svetlo siva snov ali črni preostanek. K temu sva po ohlajanju dodala vodo. Rezultate navajava v nadaljevanju.

3 REZULTATI IN DISKUSIJA

V tabeli 1 so predstavljene vse epruvete, ki sva jih pri eksperimentalnem delu uporabila, napisana je njihova sestava in s fotografijami ponazorjeno dogajanje v epruvetah, v katere sva dala koščke litija in vsebino segrevala. Na embalažah epruvet običajno ni zapisano, kaj vsebuje steklo, zato je v tabeli naveden samo tip stekla, ne pa tudi odstotna vsebnost posameznih spojin.

Ime epruvete	**Tip stekla**	**Dogajanje v epruveti ob reakciji z litijem**
Soda lime glass	natrij-kalcijevo steklo	 
Schott Fiolax	borosilikatno steklo	 

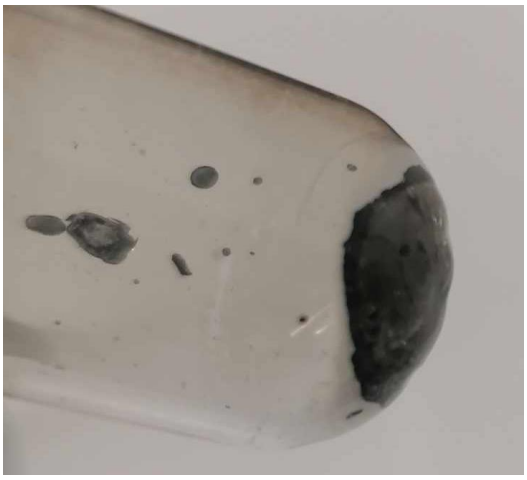
Duran	borosilikatno steklo	 
Vega 16x160	AR steklo, ki ima dodatek kalija oz. kalcija	
Vega 13x130	borosilikatno steklo	 
Assistent – soda lime glass	natrij-kalcijevo steklo	 

Boro 3.3. glass	borosilikatno steklo	 
Schott Supremax	borosilikatno steklo	
Epruveta brez napisa	natrij-kalcijevo steklo	 
Test tubes neutral	natrij-kalcijevo steklo	 

Boral	borosilikatno steklo	 

Tabela 1: Seznam epruvet, ki sva jih uporabila pri reakciji, njihova sestava in slikovni prikaz dogajanja med segrevanjem epruvete, v katero sva dodala koščke litija.

Ob uporabi nekaterih epruvet je bilo očitno, da je litij reagiral s steklom, pri drugih pa nekoliko manj. Da litij in steklo res reagirata tudi v preostalih epruvetah, ki se niso očitno stalile in počile, je najbolje vidno na spodnji sliki. Epruveta v tem delu ni gladko zaobljena, steklo je valovito (slika 1).



Slika 1: Fotografija spodnjega dela epruvete, ki je po reakciji med litijem in steklom valovita.

Po ohlajanju epruvet sva v tiste, ki so bile na videz malo poškodovane ali samo počene, dodala vodo. Opazimo nekaj mehurčkov, kar pomeni, da je nekaj litija ostalo nezreagiranega (slika 2).

Slika 2: Ko dodamo v epruveto s segretim in delno zreagiranim litijem vodo, izhajajo mehurčki. To se zgodi ob uporabi večine epruvet.

Epruveto Schoot Supremax, ki ima visoko temperaturno obstojnost in nizek razteznostni koeficient [6], sva po nekaj minutah nehala segrevati. V njej je ostala črna snov. Po ohladitvi sva dodala vodo. Glede na reakcijo sklepava, da je večina litija ostala nezreagiranega. Vodik je burno izhajal (slika 3).

Slika 3: Ostanek litija v epruveti Schott Supremax burno reagira z vodo, pri čemer nastaja vodik.

Kar ostane v epruveti po reakciji z vodo, je silicij (črna snov). Tega z epruvete ni bilo mogoče mehansko odstraniti, kar dokazuje reakcijo silicijevega dioksida iz stekla z litijem.

Slika 4: Ostanek črne snovi po reakciji z vodo v epruveti Schott Supremax.

Preizkusila sva segrevati tudi natrij, in sicer v običajni epruveti. Natrij se začne hitro taliti, opaziva krogličasto obliko staljene kovine (slika 5 levo). Produkti gorenja na zraku so različni oksidi, in sicer natrijev oksid, Na_2O, natrijev peroksid, Na_2O_2, ter natrijev superoksid, NaO_2, [7] (slika 5 desno):

$4Na + O_2 \rightarrow 2Na_2O$

$2Na + O_2 \rightarrow Na_2O_2$

$Na + O_2 \rightarrow NaO_2$

Slika 5: Ob segrevanju se natrij hitro stali (levo), nato nastanejo natrijev oksid, natrijev peroksid in natrijev superoksid (desno).

4 ZAKLJUČEK

V literaturi [2] je omenjen tudi preizkus z litij-boratnim steklom.

Borosilikatna stekla so za razliko od običajnih stekel, ki so s fizikalnega vidika slab prevodnik snovi (ionov) in toplote, dober prevodnik enega in drugega. Ob dodatku alkalijskih kovin se te lastnosti še izboljšajo [8]. Litij boratna stekla so uporabna v litijevih baterijah [9] in kot bioaktivna stekla, za katere je znano, da lahko npr. delujejo kot opornice ob poškodbah kosti, kosti dovajajo potrebne ione, ko pa se kost zaceli in jih obraste, se razgradijo. Po večurnem preizkusu izpostavljenosti litij boratnih stekel litiju, so tudi ta reagirala z njim. [2]

Ugotovila sva, da je v vseh uporabljenih epruvetah litij reagiral s steklom: v tistih, ki so namenjene delu pri nižjih temperaturah, hitreje in burneje (epruveta je hitro počila ali se je deformirala), v primeru temperaturno obstojnejših pa kasneje.

S strokovnjakom oblikovanja stekla Zvonetom Drobničem [10-12], ki še vedno deluje kot steklopihač in je bil od sedemdesetih let prejšnjega stoletja zaposlen v tovarni Vega (ta se je kasneje pridružila tovarni Iskra), sva opravila telefonski razgovor, v katerem nama je pojasnil razliko med epuvetami Vega različnih dimenzij. Tri dimenzije, ki jih imamo tudi na FNM (14 x 100, 16 x 120, 13 x 130 – vse mere so izražene v mm), so iz borosilikatnega stekla, ki ima tališče pri približno 850 °C. Četrti tip epruvet je dimenzije 16 x 160 in je iz AR stekla (natrij-kalcijevo steklo), ki ima za približno 100 °C nižje tališče. Gospod Drobnič naju je poučil tudi o barvi epruvet. Ob pogledu na epruveto proti svetlobi je opaziti, da so prve tri epruvete prozorne, četrta pa je zelenkasta, kar kaže na dodatek kalijevih oziroma kalcijevih spojin, ki znižajo kvaliteto stekla. Steklovina iz tega stekla je v laboratorijih še vedno uporabna, vendar je ne moremo uporabljati za eksperimente pri višjih temperaturah.

5 ZAHVALA

Steklopihaču Zvonetu Drobniču se zahvaljujeva za prijaznost, dragoceni čas in vse koristne informacije.

Literatura

[1] Lazarini F., Brenčič J. (1984). Splošna in anorganska kemija, DZS, Ljubljana, str. 419–422.
[2] D. R. Salmi, B. C. Bunker (1984), Glass corrosion in liquid lithium, *Sandia Report*.
[3] https://www.youtube.com/watch?v=GE-NkVqUiHs Pridobljeno 11. 1. 2024.
[4] https://www.youtube.com/watch?v=cFGejaYqM-c Pridobljeno 12. 1. 2024.
[5] https://www.yumpu.com/xx/document/read/36633769/steklo-skupnost-muzejev-slovenije Pridobljeno dne 12. 4. 2024.
[6] https://www.schott.com/en-no/products/borofloat-p1000314/product-variants Pridobljeno 20. 4. 2024.
[7] Drofenik M. (2010). Splošna in anorganska kemija, Uni založba d.o.o., Maribor, 301.

[8] Song L. et al. (2023). Structural investigation of lithium borate glasses by Raman spectroscopy: Quantitative evaluation of structural units and its correlation with density, *Journal of Non-Crystalline Solids*, *616*, 122478.
[9] S.S. Gundale et al. (2018). Improvement of ionic conductivity in $Li_{3.6}Si_{0.6}V_{0.4}O_4$ ceramic inorganic electrolyte by addition of $LiBO_2$ glass for Li ion battery application, *Electrochim. Acta*, *265*, 65–70.
[10] http://www.drustvosteklarjev.si/zvonko-drobnic/ Pridobljeno 12 .4. 2024.
[11] https://365.rtvslo.si/arhiv/vizionar-obrtnik-in-podjetnik/175029243 Pridobljeno 12. 4. 2024.
[12] https://www.rtvslo.si/zabava-in-slog/popkultura/retro/eden-zadnjih-steklopihacev-doma-me-uporabljajo-za-to-da-prijemam-vroce-stvari/572601 Pridobljeno 12. 4. 2024.

STROKOVNI PRISPEVKI

Dianoia 8 (2024) 101–113

Nekateri pomembnejši pristopi v kriptografiji
Some main approaches in cryptography

Mia Molnar, Mateja Grašič

Univerza v Mariboru, Fakulteta za naravoslovje in matematiko , Koroška cesta 160, 2000 Maribor, Slovenija

Povzetek

V članku obravnavamo nekaj zgodovinsko pomembnejših metod šifriranja, ki predstavljajo temelje danes uporabljanih kriptografskih pristopov. Vigenèrjeva šifra iz 16. stoletja je ena izmed najmočnejših zamenjalnih šifrirnih sistemov. Nemška Enigma, elektromehanska šifrirna naprava, je med drugo svetovno vojno dolgo omogočala varno komunikacijo med nemškimi silami. Diffie-Hellmanov protokol, predstavljen v drugi polovici 20. stoletja, pa omogoča varno izmenjavo šifrirnih ključev preko javnega kanala in pomeni eno pomembnejših orodij v našem digitalnem svetu. Na kratko podamo tudi osnovne informacije sodobnih kriptografskih tehnik. DES je simetrična blokovna šifra, ki jo je nadomestil varnejši AES. RSA je asimetrična metoda, ki temelji na faktorizaciji velikih števil, medtem ko ECC uporablja eliptične krivulje za zagotavljanje varnosti z manjšimi ključi.

Ključne besede: kriptografija, ključ, šifriranje, dešifriranje, Vigenèrjeva šifra, Enigma, Diffie-Hellman protokol, DES, AES, RSA, ECC

Abstract

In the article, we present some important encryption methods in history, which represent the foundations of the cryptographic approaches used today. The Vigenère cipher from the 16th century is one of the strongest substitution encryption systems ever invented. The German Enigma, an electromechanical encryption device, provided secure communication between German forces for a long time during World War II. The Diffie-Hellman protocol, introduced in the second half of the 20th century, enables the secure exchange of encryption keys over a public channel and is an important tool used in our digital world. We also outline basic information on modern cryptographic techniques. DES is a symmetric block cipher that has been replaced by the more secure AES. RSA is an asymmetric method based on the factorization of large numbers, while ECC uses elliptic curves to provide security with smaller keys.

Key words: cryptography, key, encryption, decryption, Vigenère cipher, Enigma, Diffie-Hellman protocol, DES, AES, RSA, ECC

1 Uvod

Namen članka je prikazati nekatere pomembnejše pristope v posredovanju skrivnih informacij, osnova katerih je proces, ki ga imenujemo *šifriranje* ali *kodiranje*. V preteklosti je bil v proces šifriranja in dešifriranja podatkov vključen relativno ozek krog ljudi (npr. v varnostnem in vojnem delovanju), v času velike digitalizacije (informacijske dobe), ki smo ji priča, pa se na (varno) prenašanje šifriranih podatkov zanašamo ob vsaki uporabi računalnika–nenazadnje tudi ves računalniški svet temelji na algoritmih in podatkih, predstavljenih (kodiranih) zgolj z uporabo števil 0 in 1.

Razvoj računalnika ima svoje zametke v času druge svetovne vojne, ko so vpletene vojne sile iskale najboljše načine šifriranja svojih komunikacij s skrivnimi podatki, ter načinov prestrezanja in dešifriranja komunikacije s podatki drugih. Enega od pomembnejših

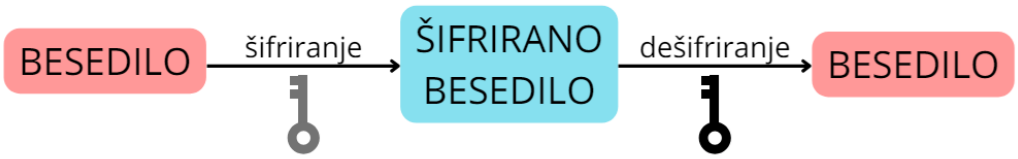
E-mail naslovi: mia.molnar@student.um.si (Mia Molnar), mateja.grasic@um.si (Mateja Grašič)

prebojev v tedanji kriptoanalizi pomeni razvoj dešifrirne tehnologije in dešifrirnih elektromehanskih naprav. Zelo znamenite so Turingove bombe (orig. Turing's bombes), s katerimi so Britanci strli enega najmočnejših sistemov šifriranja v zgodovini, nemško Enigmo, in Kolos (orig. Colossus), s katero so si pomagali pri uspešnem dešifriranju Lorenzove šifre, izjemne kodirne tehnologije, temelječe na sistemu Enigme, vendar veliko kompleksnejše, uporabljane za skrivno komunikacijo nemških vodilnih oseb s svojimi generali. V poglavju 2.2 podamo kratek pregled osnovnih dejstev o delovanju in lastnostih Enigme ter opišemo pristop k uspešnemu dešifriranju tega zapletenega šifrirnega sistema.

Kriptografija je veja matematike in računalništva, katere namen ni skriti obstoj sporočila, ampak skriti njegov pomen, proces, znan kot *šifriranje*. Beseda *kriptografija* izhaja iz grške besede *kryptós*, kar pomeni *skrit*, in *graphia*, kar pomeni *pisati*. *Kriptoanaliza* je nasprotje kriptografiji in se ukvarja z dešifriranjem skritega besedila brez predhodno poznanega ključa in metode šifriranja.

Šifrirni postopek (slika 1) vključuje algoritem in ključ. Ključ je vrednost, neodvisna od besedila. Za šifriranje besedila ga pošiljatelj pošlje skozi šifrirni algoritem. Algoritem je splošen sistem za šifriranje in ga je treba natančno določiti z izbiro ključa. Šifrirni algoritem bo ustvaril različno šifrirano besedilo, odvisno od specifičnega ključa, ki se uporablja v določenem trenutku. Sprememba ključa spremeni izhod algoritma. S pomočjo dešifrirnega algoritma in ustreznega ključa se lahko šifrirano besedilo spremeni nazaj v izvirno besedilo.

Temeljni koncept današnje kriptografije je *Kerckhoffov princip*, ki pravi, da varnost kriptografskega sistema ne sme biti odvisna od skrivnosti algoritma, ampak zgolj od skrivnosti ključa. Dober kriptografski sistem mora tako ostati varen tudi, če je njegov algoritem znan.



Slika 1: Šifrirni postopek.

V kriptografiji se uporabljajo različni postopki za šifriranje podatkov. Eden osnovnih postopkov je *transpozicija*, pri kateri zgolj zamenjamo položaje znakov sporočila, jih permutiramo. Za zelo kratka sporočila je ta metoda negotova, saj obstaja le omejeno število načinov preurejanja končnega števila znakov. Drug osnovni postopek je *zamenjava*, kjer vsak znak besedila zamenjamo z drugim znakom. Pri transpoziciji vsak znak ohrani svojo identiteto, vendar spremeni svoj položaj, medtem ko pri zamenjavi vsak znak spremeni svojo identiteto, vendar ohrani svoj položaj. Pogosto oba omenjena osnovna postopka tudi kombiniramo. Drugo poglavje je namenjeno predstavitvi dveh zgodovinsko pomembnih zamenjalnih šifrirnih sistemov. Eden je že omenjena Enigma, v poglavju 2.1 pa predstavimo Vigenèrjevo šifriranje, ki je svojo skrivnost ohranjalo dolga tri stoletja.

Glede na kriterij uporabljenih ključev lahko kriptografijo delimo na simetrično in asimetrično. Prikaz delovanja nekaterih takih kriptografskih metod podamo v tretjem poglavju. *Simetrična kriptografija* uporablja enak ključ za šifriranje in dešifriranje sporočil, osnovna zahteva pa je ohranitev tajnosti tega ključa, kar pomeni osnovni problem tega pristopa. Primera simetričnih kodirnih sistemov sta DES (Data Encryption Standard) in AES

(Advanced Encription Standard). Pri *asimetrični* (ali *javni*) *kriptografiji* se za šifriranje in dešifriranje uporabljata dva ključa: javni in tajni ključ. Asimetrična kriptografija problem deljenja ključev šifrirnega algoritma reši z uporabo javnih ključev, ki se delijo med uporabnike, za dešifriranje pa uporablja kombinacijo javnega in tajnega ključa. Ta metoda je počasnejša od simetrične, zahtevnejša in uporablja mnogo daljše ključe kot simetrična kriptografija.

V poglavju 3.1 predstavimo delovanje asimetričnega šifriranja na primeru Diffie-Hellmanovega protokola izmenjave ključev. Ta matematična metoda podaja algoritem za varno izmenjavo šifrirnih ključev preko javnega kanala.

V poglavju 3.2 podamo kratek opis nekaterih pomembnih simetričnih in asimetričnih pristopov v aktualnih informacijskih tehnologijah. Z njihovo pomočjo so npr. digitalno podpisovanje dokumentov, digitalna identiteta, spletno nakupovanje ter spletno bančništvo postali nepogrešljivi in precej varen del našega vsakodnevnega delovanja.

2 Pomembnejša zamenjalna šifrirna sistema

V tem poglavju predstavimo delovanje Vigenèrjeve šifre in Enigme, ki sodita med pomembnejše zgodovinske pristope v kriptografiji. Spadata med simetrične zamenjalne šifrirne sisteme, kar pomeni da za šifriranje in dešifriranje uporabljata enak ključ in sporočila pretvorita na zamenjalni način.

2.1 Vigenèrjeva šifra

Pričnimo z enostavno zamenjalno metodo šifriranja. Cezarjeva šifra je preprost način kodiranja, ki jo je v 1. stoletju pred našim štetjem uporabljal Julij Cezar za skrito komunikacijo s svojimi generali. To šifriranje temelji na translaciji črk abecede za izbrano število mest, recimo p. Če zaporedoma vse črke slovenske abecede označimo s števili od 0 do 24 (tabela 1), potem lahko kodiranje posameznih črk opišemo z uporabo kongruenc. Tako šifriranje črke, ki jo označuje $n \in \{0, \ldots, 24\}$, podaja funkcija

$$E(n) = (n + p) \bmod 25,$$

dešifriranje zakodirane črke $m \in \{0, \ldots, 24\}$ pa funkcija

$$D(m) = (m - p) \bmod 25.$$

A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Tabela 1: Identifikacija črk s številkami.

Opazimo, da morata šifrirna funkcija E in dešifrirna funkcija D zadoščati osnovni zvezi $D(E(n)) = D(n+p) \bmod 25 = ((n+p)-p) \bmod 25 = n$ za vsak n. S tem ima funkcija D lastnost, da prevede šifrirano besedilo. Podobno je $E(D(m)) = m$ za vsak m, torej sta si funkciji E in D inverzni.

Na primer, z izbiro besedila 'ZNANJE JE MOČ' (presledkov med besedami pri šifriranju ne upoštevamo) in premika za $p = 7$ mest je zašifrirano besedilo enako 'EUGURLRLTVJ'.

Ker se s to metodo izbrana črka vedno preslika v isto črko (določeno z izbiro števila p), je z analizo frekvenc pojavljanja posameznih črk v besedilu in poznavanjem lastnosti jezika (najpogosteje in najredkeje uporabljane črke) zlahka ugotoviti izbrani p, ki je ključ Cezarjeve šifre.

Vigenèrjeva šifra je metoda kodiranja iz sredine 16. stoletja, ki za šifriranje sporočila uporablja 25 različnih šifrirnih abeced (v primeru slovenske abecede). V uporabi je bila vse do druge polovice 19. stoletja. Prvi korak pri šifriranju je izdelava Vigenèrjevega kvadrata, kot je prikazano v tabeli 2. Vsaka vrstica predstavlja eno od šifrirnih abeced za Cezarjevo šifriranje, kjer se vsaka naslednja abeceda premakne za eno črko v levo glede na abecedo v prejšnji vrstici.

Prvi stolpec Vigenèrjevega kvadrata predstavlja črke ključa, prva vrstica pa črke besedila, ki ga želimo zakodirati.

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
A	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
B	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
C	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
Č	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
Š	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
T	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
U	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
V	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
Z	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
Ž	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z

Tabela 2: Vigenèrjev kvadrat.

Za uporabo Vigenèrjevega kvadrata moramo imeti predhodno določen ključ. Daljši kot je ključ, večja je kompleksnost šifriranja. Če je dolžina ključa krajša od dolžine besedila, se ključ ponavlja periodično. V našem primeru, če je besedilo 'ZNANJE JE MOČ' in je ključ 'METULJ', se ključ uporablja periodično na način, prikazan v tabeli 3.

Besedilo	Z	N	A	N	J	E	J	E	M	O	Č
Ključ	M	E	T	U	L	J	M	E	T	U	L

Tabela 3: Periodična uporaba ključa.

Za šifriranje prve črke besedila, Z, narišemo navpično črto črke Z, in nato horizontalno črto iz prve črke ključa, M. Presek bo prva črka šifriranega besedila, K, kot lahko vidimo v tabeli 4. Postopek ponovimo za vsako črko besedila. Pri dešifriranju v vrstici črke ključa poiščemo črko šifriranega besedila in pogledamo, v stolpcu katere črke besedila se nahaja.

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
A	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
B	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
C	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
Č	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M

Tabela 4: Uporaba Vigenèrjevega kvadrata.

Vigenèrjevo šifriranje lahko zapišemo s funkcijama E in D. Vsako črko predstavimo s številko, kot prikazuje tabela 1. Identifikacijo s številkami na našem primeru prikazuje tabela 5.

Besedilo	Z	N	A	N	J	E	J	E	M	O	Č
Besedilo s številkami	23	14	0	14	10	5	10	5	13	15	3
Ključ	M	E	T	U	L	J	M	E	T	U	L
Ključ s številkami	13	5	20	21	12	10	13	5	20	21	12
Šifrirano besedilo	K	Š	T	J	V	O	Z	J	H	K	O
Šifrirano besedilo s številkami	11	19	20	10	22	15	23	10	8	11	15

Tabela 5: Rezultat šifriranja.

Poglejmo si matematični opis zgoraj predstavljenega postopka na besedilnem primeru. Vsako besedilno sporočilo lahko predstavimo v obliki končnega zaporedja števil od 0 do 24, ki predstavljajo zaporedne črke sporočila. Dolžina tega zaporedja je enaka številu znakov v besedilu. Z besedo zaporedje bomo tako imeli v mislih končno zaporedje. Naj bo $K = (k_1, k_2, \ldots, k_d)$ zaporedje, ki pripada črkam ključa, in $B = (b_1, b_2, \ldots, b_n)$ zaporedje, ki pripada črkam besedila, predstavljenih s številkami. Za vsak $i = 1, \ldots, d$ definirajmo i-to šifrirno funkcijo $f_i : B \to \{0, 1, \ldots, 24\}$ odvisno od izbire ključa K, s predpisom

$$f_i(b) = (b + k_i) \bmod 25 \text{ za vsak } b \in B.$$

Tedaj je $f_i^{-1}(b) = (b - k_i) \bmod 25$, za vsak $b \in B$, inverzna funkcija funkcije f_i. Opazimo lahko, da v definiciji funkcije f_i nastopa Cezarjeva zamenjalna metoda za $p = k_i$. Naj zaporedje $Z = (z_1, z_2, \ldots, z_n)$ pripada zakodiranemu besedilu. Besedilo šifriramo s funkcijo $E_K : B \mapsto Z$ s pripadajočim ključem K, s predpisom

$$E_K(b_j) = f_{(j-1) \bmod d+1}(b_j) \text{ za vsak } j = 1, \ldots, n,$$

in dešifriramo s funkcijo $D_K : Z \mapsto B$, s predpisom

$$D_K(z_j) = f^{-1}_{(j-1) \bmod d+1}(z_j) \text{ za vsak } j = 1, \ldots, n.$$

ALGORITEM Vigenèrjevo šifriranje (besedilo, ključ, m)
{Algoritem zašifrira besedilo in rezultat vrne v parametru zakodiranoBesedilo. Vhodni podatek m predstavlja število črk v abecedi (v našem primeru je to 25).}
začni
ključSŠtevilkami = pretvori črke v število (ključ);
besediloSŠtevilkami = pretvori črke v število (besedilo);
n = preberi dolžino (besedilo);
za $i = 1$ do n naredi
$s_i = E_K(b_i)$;
zakodiranoBesedilo = pretvori števila v črke ($s_1 s_2 \ldots s_n$);
konec.

Vigenèrjeva šifra se izkaže za učinkovito predvsem zato, ker iste črke ne kodira vedno enako. Zaradi tega je neobčutljiva na analizo frekvenc pojavljanja posameznih črk. Njena slabost je ponavljajoči se ključ. Če kriptoanalitik pravilno ugane dolžino ključa, ga lahko obravnava kot več prepletajočih se Cezarjevih šifer, ki pa jih je lahko razbiti. Z uporabo ključa približno enake dolžine kot besedilo se lahko temu izognemo.

2.2 Razvoj šifrirnih naprav–od šifrirnih diskov do Enigme

Najstarejši kriptografski stroj je šifrirni disk, ki ga je v 15. stoletju izumil italijanski arhitekt Leon Battista Alberti. Sestavljen je iz dveh bakrenih koncentričnih diskov različnih velikosti. Na vsakem je na robu vgrajena abeceda, pri čemer je na zunanjem disku standardna abeceda, na notranjem disku pa izbrana šifrirna abeceda. Šifriranje z diskoma je določeno z izbiro (začetne) nastavitve diskov in temelji na Cezarjevih premikih.

Leta 1918 sta Arthur Scherbius in Richard Ritter ustanovila podjetje Scherbius & Ritter, specializirano za inovativne inženirske rešitve. Razvila sta Enigmo, električno različico Albertijevega šifrirnega diska, ki je postala eden najmočnejših sistemov šifriranja v zgodovini. Uporabljali so jo Nemci v času druge svetovne vojne. V osnovi Scherbiusov izum vključuje tri med seboj povezane elemente: tipkovnico za vnos posameznih črk besedila, mešalno enoto iz več kolutov s šifrirnimi abecedami, ki šifrira vsako črko besedila v ustrezno črko šifriranega besedila, in prikazno ploščo z lučkami, kjer se prikazujejo črke šifriranega besedila. Šifriranje določa začetna postavitev kolutov, pri vsakem vnosu črke besedila pa se dodatno eden od kolutov premakne za eno mesto, zato je vsaka črka besedila kodirana s svojo šifrirno abecedo po metodi Cezarjevega šifriranja.

V osnovni različici Enigme nastopajo trije koluti, vsak ima 26 možnih začetnih orientacij (toliko je črk nemške abecede). Zato je skupno število možnih začetnih nastavitev orientacije kolutov enako

$$26 \cdot 26 \cdot 26 = 17.576.$$

Koluti so odstranljivi in zamenljivi, kar dodatno vpliva na šifrirni algoritem. Tri kolute (označimo jih z 1, 2 in 3) lahko razporedimo na 6 načinov, in sicer

$$123, 132, 213, 231, 312, 321.$$

Za še dodatno povečanje števila šifrirnih abeced je v osnovni različici Enigme dodan tudi vtični blok med tipkovnico in prvim kolutom, ki omogoča uporabniku, da vstavi kable, ki premešajo nekatere črke, preden vstopijo v mešalno enoto. Na primer, če kabel povezuje

črki A in B, se črka A šifrira kot B in obratno. V osnovni različici je imel uporabnik na voljo šest kablov, s katerimi je lahko zamenjal šest parov črk, medtem ko je štirinajst črk ostalo nepovezanih. Med 26 vtičnicami lahko izberemo 12 črk, ki bodo povezane s kabli. To naredimo na $\binom{26}{12}$ načinov. Treba je še določiti, na koliko različnih načinov lahko 6 kablov poveže 12 izbranih vtičnic. Prvi konec prvega kabla vstavimo v eno izmed izbranih vtičnic. Za drugi konec prvega kabla imamo nato 11 možnosti izbire vtičnice. Nato začetek drugega kabla vključimo v poljubno še neizbrano vtičnico in za drugi konec izberemo eno od 9 preostalih vtičnic. Tako nadaljujemo, dokler za povezavo črk šestega kabla ne ostane le en par črk. Tako je skupno število načinov, kako povežemo 12 vtičnic s 6 kabli, enako

$$11 \cdot 9 \cdot 7 \cdot 5 \cdot 3 \cdot 1 = 11!!$$

Skupno število različnih možnih povezovanj izračunamo kot produkt števila možnih izbiranj vtičnic in števila načinov njihovega povezovanja:

$$\binom{26}{12} \cdot 11!! = \frac{26!}{14! \cdot 6! \cdot 2^6} = 100.391.791.500.$$

Število vseh začetnih nastavitev osnovne različice Enigme je zato enako

$$100.391.791.500 \cdot 17.576 \cdot 6 = 1,0586917 \cdot 10^{16},$$

kar je približno 10.000.000.000.000.000. Z dodajanjem kablov in kolutov v sistem Enigme se število začetnih kombinacij lahko poljubno poveča.

Za tajno prenašanje podatkov z Enigmo je bilo treba poznati nastavitev kolutov in kablov vtičnega bloka, t. i. dnevni ključ, ki je ključ tega simetričnega šifrirnega postopka. Glede na zgornje izračune je možnih izbir ključa v osnovni različici Enigme približno 10^{16}. Sprva so Nemci uporabljali dnevni ključ za šifriranje vseh sporočil istega dne, seznam dnevnih ključev pa je vsebovala t. i. knjiga kod. Na primer, prvi dan v mesecu bi knjiga kod določila naslednji dnevni ključ:

nastavitve kablov: M/S - T/A - P/V - R/F - U/C - B/X,

vrstni red kolutov: 3-1-2,

orientacija kolutov: A-M-S.

Skrivno besedilo so na napravi Enigma z upoštevano dnevno nastavitvijo šifrirali, šifrirano besedilo so preko radia sporočili prejemniku, ki je lahko z uporabo Enigme, nastavljene na isti dnevni ključ, dešifriral sporočilo. Šibkost tega pristopa je šifriranje velike količine sporočil z uporabo istega ključa.

Nemci so za dodatno varnost uporabljali enkratni sporočilni ključ, pri njegovem prenosu pa so si pomagali z dnevnim ključem. Sporočilni ključ je imel enake nastavitve kablov in vrstni red kolutov kot dnevni ključ, vendar drugačno orientacijo kolutov. Pošiljatelj je svoj stroj nastavil v skladu z dnevno kodo (npr. z orientacijo FNR) in nato naključno izbral novo orientacijo kolutov za sporočilni ključ (npr. LSP). Sporočilni ključ je nato zakodiral glede na dnevni ključ in ga dvakrat vtipkal v stroj Enigma. Na primer, pošiljatelj je zakodiral sporočilni ključ LSPLSP kot KTVPAM. Nato bi spremenil svoj stroj na nastavitev LSP in zašifriral sporočilo. Prejemnik bi prejel sporočilo in ga vnesel v svoj stroj, nastavljen na dnevni ključ FNR. Prvih šest črk prejetega sporočila, KTVPAM, bi razkrilo sporočilni ključ LSPLSP. Prejemnik bi svoje kolute nastavil na orientacijo LSP in dešifriral sporočilo.

2.2.1 Dešifriranje Enigme

Poljski matematik Marian Adam Rejewski je s svojimi ugotovitvami postavil temelje za dešifriranje Enigme. Vsak dan je prejemal nova prestrežena sporočila, ki so se vsa začela s šestimi črkami, določenimi z enkratnim tročrkovnim sporočilnim ključem, zašifriranim po dnevni kodi. Na primer, prejel je štiri sporočila, ki so se vsa začela z zašifriranimi sporočilnimi ključi, prikazanimi v tabeli 6.

	1. črka	2. črka	3. črka	4. črka	5. črka	6. črka
1. sporočilo	B	K	L	T	J	M
2. sporočilo	S	A	G	I	Z	H
3. sporočilo	N	E	T	R	P	C
4. sporočilo	O	U	V	F	D	K

Tabela 6: Prikaz sporočilnih ključev.

V vsakem sporočilu sta 1. in 4. črka šifriranji iste črke, tj. prve črke sporočilnega ključa. Prav tako sta 2. in 5. črka ter 3. in 6. črka šifriranji iste črke. Razlog za različno šifriranje iste črke je premik koluta za tri korake med obema šifriranjema. Z vsakim novim prestreženim sporočilom lahko odkrijemo dodatne vzorce med 1. in 4. črko, 2. in 5. črko ter 3. in 6. črko. V tabeli 6 drugemu sporočilu ustreza povezava med črkama S in I, tretjemu med črkama N in R ter četrtemu med O in F. Te povezave lahko predstavimo s pari (B,T), (S,I), (N,R) in (O,F), tabela 7.

1. črka	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4. črka		T												R	F				I							

Tabela 7: Abeceda odnosov.

Z dovolj prestreženimi sporočili v enem dnevu je lahko do konca izpolnil abecedo odnosov. Primer prikazuje tabela 8.

1. črka	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4. črka	H	T	V	J	M	K	Z	B	C	S	N	G	U	R	F	D	Y	X	I	A	W	P	E	O	L	Q

Tabela 8: V celoti izpolnjena abeceda odnosov.

Rejewski je odkril vzorce med povezavami črk. Identificiral je verige povezanih črk, cikle in njihovo dolžino ter enako storil za druge pare črk. Naš primer za povezavo med 1. in 4. črko lahko zapišemo v obliki ciklov

$$(AHBT)(CVPDJSI)(EMUW)(FKNRXO)(GZQYL).$$

Preštejemo lahko število ciklov in število elementov v vsakem od njih. Rejewski je ugotovil, da se število povezav v verigah (dolžine ciklov) ne spremeni, če spremenimo nastavitve kablov. Število povezav v verigah je torej posledica nastavitev kolutov.

Število nastavitev kolutov je enako produktu možnih kombinacij orientacije kolutov, 17.576, in vrstnega reda kolutov, 6, skupaj 105.456. Rejewski se je tako namesto problema, katera od 10^{16} kombinacij je pravilna, ukvarjal z vprašanjem, katera od 105.456 nastavitev je bila povezana s številom povezav v nizu verig.

S svojo ekipo je Rejewski na replikah Enigma strojev pregledal vsako izmed 105.456 nastavitev kolutov, beležil dolžine verig in sestavil katalog. Katalogizacija je trajala eno leto, po tem pa so lahko začeli razkrivati šifro Enigme.

Za dešifriranje je bilo treba vsak dan preveriti prvih šest črk zakriptiranih ključev vseh prestreženih sporočil, sestaviti tabele odnosov, s pomočjo katerih so določili verige in število povezav v vsaki. Nato so z uporabo kataloga poiskali vnos, ki je vseboval pravilno število verig z ustreznim številom povezav v vsaki, in tako ugotovili nastavitve kolutov za dnevni ključ.

Preostala je še naloga določitve nastavitve kablov. Do tega so prišli tako, da so upoštevali nastavitve kolutov, odstranili vse kable iz priključne plošče in vnesli del prestreženega šifriranega besedila v stroj Enigma. Občasno so se pojavile rahlo prepoznavne fraze, na podlagi katerih so se lahko uganile nastavitve kablov. Z upoštevanjem vseh nastavitev se je pridobil celoten dnevni ključ, ki so ga lahko uporabili za dešifriranje sporočil, poslanih tisti dan.

3 Nekatere novejše metode v kriptografiji

V poglavju se posvečamo nekaterim novejšim kriptografskim metodam. Diffie-Hellmanov protokol je namenjen varni izmenjavi ključa preko javnega kanala in reši problem tajnosti ključa, ki je ena od glavnih težav v 2. poglavju predstavljenih pristopov. Opišemo tudi nekatere trenutno uporabljane simetrične in asimetrične šifrirne tehnike.

3.1 Protokoli za dogovor/izmenjavo ključev

Protokoli za dogovor/izmenjavo ključev so metode, ki omogočajo generiranje tajnega skupnega ključa uporabnikov preko javnega kanala z uporabo javnega ključa. Dobljen tajni ključ je nato uporabljen v katerem od aktualnih simetričnih pristopov šifriranja. Eden izmed teh je Diffie-Hellmanov protokol, ki sta ga prvič objavila Whitfield Diffie in Martin Hellman leta 1976.

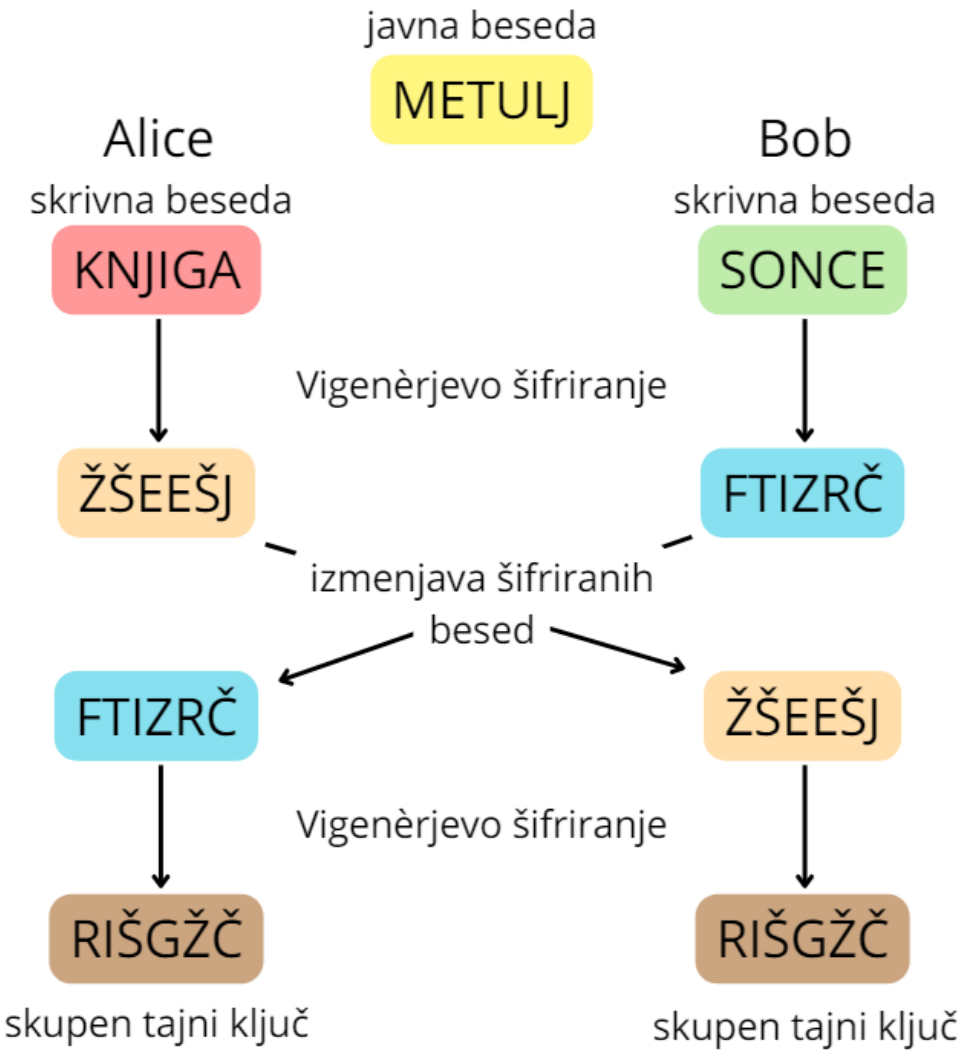
Opišimo varno izmenjavo tajnega ključa med dvema osebama (v kriptografiji namišljena lika Alice in Bob) preko javnega kanala. Sam Diffie-Hellmanov protokol temelji na diskretnem logaritmu v multiplikativni grupi končnih polj, v našem primeru pa bodo uporabljeni pristopi iz prejšnjih poglavij. Glavna ideja metode je, da imata Alice in Bob vsak svojo skrivno informacijo, ki jo z izbrano šifrirno metodo združita v skupen tajni ključ TK. Gre za enega prvih pristopov, katerega efektivnost temelji na delovanju enosmerne funkcije. Funkcija f iz množice X v množico Y s predpisom $y = f(x)$ za vsak $x \in X$ je *enosmerna*, če je izračun $y = f(x)$ lahko izvedljiv (v polinomski časovni zahtevnosti), medtem ko njen inverz $x = f^{-1}(y)$ bodisi ne obstaja bodisi je težko izračunljiv.

Koraki poteka algoritma izmenjave ključa so naslednji:

1. *Določitev javne informacije J in funkcije šifriranja E_K, kjer K predstavlja ključ za šifriranje.*
2. *Izbira skrivnih informacij A in B za funkcijo šifriranja E_K.*
3. *Šifriranje J z izbrano funkcijo E_K in ključema A in B*
   $\Rightarrow$ Alice: $E_A(J)$, Bob: $E_B(J)$.
4. *Izmenjava šifriranih skrivnih informacij $E_A(J)$ in $E_B(J)$.*
5. *Šifriranje $E_A(J)$ in $E_B(J)$ z izbrano funkcijo E_K*
   $\Rightarrow$ Alice: $E_A(E_B(J))$, Bob: $E_B(E_A(J))$.

6. *Tvorjen skupen tajni ključ* $TK = E_A(E_B(J)) = E_B(E_A(J))$.

Dobljen ključ TK nato Alice in Bob uporabljata za šifriranje in dešifriranje sporočil med njima.



Slika 2: Primer protokola za dogovor o ključu.

V našem primeru se dogovorita, da bosta za generiranje tajnega ključa uporabila Vigenèrjevo šifriranje in javno besedo 'METULJ'. Slika 2 prikazuje primer poteka algoritma.

Ključna lastnost metod za izmenjavo ključev je ta, da tudi če napadalec prestreže vse izmenjane informacije med osebama, ne more izračunati skupnega tajnega ključa, če ne pozna skrivnih vrednosti A in B. To zagotavlja varnost komunikacije med osebama.

ALGORITEM Izmenjava ključa (javnaBeseda, A, B)
{Algoritem ustvari skupen tajni ključ brez razkritja podatkov A in B ter ga vrne v parametru skupenTajniKljuč.}
začni
AlicinRezultat = Vigenèrjevo šifriranje (javnaBeseda, A, 25);
BobovRezultat = Vigenèrjevo šifriranje (javnaBeseda, B, 25);
ApošljeB = AlicinRezultat; {Alice pošlje svoj rezultat Bobu.}
BpošljeA = BobovRezultat; {Bob pošlje svoj rezultat Alice.}
novAlicinRezultat = Vigenèrjevo šifriranje (BpošljeA, A, 25);
novBobovRezultat = Vigenèrjevo šifriranje (ApošljeB, B, 25);
skupenTajniKljuč = novAlicinRezultat = novBobovRezultat;
konec.

V Diffie-Hellmanovem protokolu algoritem uporablja funkcijo $E(x) = N^x \bmod P$. Alice in Bob skupaj izbereta praštevilo P in naravno število N, ki je primitivni koren po modulu P. Ti števili nista skrivni, Alice in Bob pa morata izbrati svoji skrivni števili a in b. Tajni ključ je oblike $TK = N^{ab} \bmod P$. Varnost protokola je odvisna od pravilne izbire začetnih parametrov N in P. Ti števili morata biti naključni, P dolžine vsaj 600 mest, N pa je lahko majhen. Varnost Diffie-Hellmanovega protokola temelji na računskem problemu iz teorije števil, imenovanem problem diskretnega logaritma. Opišemo ga lahko na naslednji način. Naj bo G končna multiplikativna ciklična grupa z n elementi, kjer je n praštevilo. Naj bo c generator grupe G. Potem lahko vsak element $g \in G$ zapišemo kot $g = c^k$ za neko naravno število k. Funkcija diskretnega logaritma z osnovo c, $log_c : G \to \mathbb{Z}_n$, vsakemu elementu g priredi enolično določen eksponent k po modulu n. Ta funkcija je izomorfizem med grupo G in $\mathbb{Z}_n$ (množico ostankov pri deljenju z n). Da bi napadalec ogrozil varnost, bi moral problem diskretnega logaritma rešiti, za njega pa trenutno ni znan učinkovit splošen algoritem na standardnih računalnikih.

3.2 Osnovno o DES, AES, RSA in ECC

DES (Data Encryption Standard) je simetrična blokovna šifrirna metoda, ki je v širšo uporabo stopila leta 1977 kot izbrani standard za obdelavo informacij v ZDA. V algoritmu bloki dolžine 64 bitov besedila vstopijo v proces šifriranja in so pretvorjeni v 64-bitne bloke šifriranega besedila. Šifriranje je sestavljeno iz več faz in vključujejo preoblikovanje ključev, razširitveno permutacijo in substitucijo. Dolžina osnovnega ključa je 56 bitov, v posamezni fazi šifriranja pa se uporabijo 48-bitni ključi, ki so dobljeni iz osnovnega. Podrobneje je postopek opisan v [12]. Za dešifriranje se uporablja isti ključ in algoritem, le v obratni smeri.

Priljubljenost DES se je zmanjšala zaradi odkritih ranljivosti, ki omogočajo razvoj učinkovitih napadov. Sledil je razvoj TDES, DES-X in drugih modifikacij. Leta 2001 se je kot nov standard za prenos informacij izbral AES (Advanced Encryption Standard), saj zagotavlja večjo varnost. To je simetrični kriptografski algoritem za šifriranje podatkov, ki uporablja ključe dolžine 128, 192 ali 256 bitov. AES šifrira podatke v blokih po 128 bitov in uporablja isti ključ za šifriranje in dešifriranje. Razbitje 128-bitne šifre bi po trenutnih ocenah lahko trajalo milijone let, medtem ko bi kvantni računalniki za razbitje te šifre potrebovali do šest mesecev. Več podrobnosti o AES lahko najdemo v [1].

Trenutno zelo aktualen algoritem je RSA, ki so ga leta 1977 opisali R. Rivest, A. Shamir in L. Adleman. Spada v skupino asimetričnih kriptografskih metod, za razliko od opisanega protokola Diffie-Hellman pa se RSA algoritem uporablja tudi za šifriranje in dešifriranje informacij. Pri šifriranju je uporabljen javni ključ in postopek šifriranja je dostopen vsakomur. Za dešifriranje je potreben tajni ključ, zato je to omogočeno zgolj izbranim uporabnikom. Javni ključ se ustvari z množenjem dveh velikih praštevil p in q, pri čemer je produkt $n = p \cdot q$ prvi del javnega ključa, drugi del pa poljubno število e, tuje s $(p-1)(q-1)$. Tajni ključ sestavljata število n in inverz števila e po modulu $(p-1)(q-1)$. Več informacij lahko preberete v [10]. Varnost RSA izhaja iz kompleksnosti problema faktorizacije velikih števil. Medtem ko je iskanje velikih praštevil razmeroma enostavno, je razčlenjevanje velikih števil na produkt teh praštevil izjemno zahtevno in praktično neizvedljivo.

Šifre z javnimi ključi temeljijo na težavnosti določenih matematičnih problemov, kot je faktorizacija celih števil, ki so časovno zahtevni za reševanje. Zato morajo biti asimetrični ključi daljši od simetričnih, da nudijo enako varnost. 1024-bitni RSA ključi so po moči enakovredni 80-bitnim simetričnim ključem, 2048-bitni RSA ključi so primerljivi s 112-bitnimi simetričnimi ključi, 3072-bitni s 128-bitnimi in 15.360-bitni RSA ključi so enakovredni 256-bitnim simetričnim ključem.

Eliptična kriptografija (Eliptic Curve Cryptography oz. ECC) je oblika kriptografije z javnimi ključi, ki uporablja matematične lastnosti eliptičnih krivulj. Eliptična krivulja je opisana z enačbo $y^2 = x^3 + ax + b$, kjer sta a in b konstanti, za definicijsko območje pa izberemo končno polje. Varnost kriptografskega sistema je povezana z zahtevnostjo reševanja diskretnega logaritma na eliptični krivulji. ECC zagotavlja enako varnost kot klasične kriptografske metode, a z manjšimi ključi, kar omogoča varnejšo in učinkovitejšo rabo prostora ter manjšo porabo energije. Na primer, 313-bitni ključ z eliptičnimi krivuljami nudi enako varnost kot 4096-bitni RSA ključ. Poleg tega ECC pogosto uporablja hitrejše in učinkovitejše operacije v primerjavi z RSA. Več o postopku šifriranja na [4].

4 Zaključek

V zaključku lahko ugotovimo, da različne kriptografske metode ponujajo različne ravni varnosti in kompleksnosti. Vigenèrjeva šifra, čeprav zgodovinsko pomembna, danes ne zagotavlja zadostne zaščite zaradi naprednih tehnik za analizo. Enigma je bila kljub svoji kompleksnosti prelomljena z analitičnimi pristopi in močjo človeškega uma. Diffie-Hellmanov protokol pa predstavlja ključni mejnik v sodobni kriptografiji, saj omogoča varno izmenjavo ključev, kar je osnova za številne varnostne rešitve v današnjem digitalnem svetu. Povezava med izmenjavo šifriranih vrednosti in enosmernimi funkcijami zagotavlja varnost kljub prenosu preko javnih kanalov. Poleg tega smo predstavili osnovne informacije o sodobnih kriptografskih tehnikah. DES, simetrični blokovni šifrirni algoritem, je bil nadomeščen z AES za izboljšano varnost z daljšimi ključi. RSA, asimetrična metoda, temelji na težavnosti faktorizacije velikih števil, medtem ko prav tako asimetrična metoda ECC uporablja eliptične krivulje za doseganje visoke ravni varnosti z uporabo manjših ključev. Razumevanje teh metod nam omogoča boljše razumevanje razvoja varnosti podatkov in zaščite komunikacij v sodobnem času.

Literatura

[1] Advanced Encryption Standard (AES), `https://medium.com/@marketing_14184/advanced-encryption-standard-aes-dfb758ecbfa0`

[2] W. Diffie and M. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22(6):644–654, 1976.

[3] J. Katz, Y. Lindell, *Introduction to Modern Cryptography, Second Edition*, CRC Press, 2015.

[4] L. Klusaitė, What is elliptic curve cryptography?, https://nordvpn.com/blog/elliptic-curve-cryptography/

[5] N. Krzyworzeka, Asymmetric cryptography and trapdoor one-way functions, *Automatyka* **2**, vol. 20 (2016), 39–51. http://dx.doi.org/10.7494/automat.2016.20.2.39

[6] B. Petelinek, Diskretni logaritem, https://dk.um.si/Dokument.php?id=14715&lang=slv

[7] K. Prasad, M. Kumari, A review on mathematical strength and analysis of Enigma, arXiv:2004.09982v1.

[8] B. Sankhyan, A. Baliyan, A. Kumar, Review on Symmetric and Asymmetric Cryptography, *IJRASET* **12**, III (2024), 2934–2940.

[9] S. Singh, *The Code Book : The Secret History of Codes and Code-Breaking*, Fourth Estate, London, 1999.

[10] T. Šavs, RSA kriptiranje, http://pefprints.pef.uni-lj.si/1800/1/Savs_Teja-RSAkriptiranje.pdf

[11] M. Tarawneh, Cryptography: Recent Advances and Research Perspectives, http://dx.doi.org/10.5772/intechopen.111847

[12] S. Upadhyay, Data encryption standard (DES) | Set 1, https://www.geeksforgeeks.org/data-encryption-standard-des-set-1

Dianoia 8 (2024) 115-126

A brief analysis of the inclusion of environmental topics in the first and second degree pedagogical study programmes of Slovenian universities

Kratka analiza vključevanja okoljskih tem v študijske programe prve in druge stopnje pedagoških programov slovenskih univerz

Maja Kerneža, Dejan Zemljak

University of Maribor, Faculty of Education, Koroška cesta 160, 2000 Maribor
University of Maribor, Faculty of Natural Sciences and Mathematics, Koroška cesta 160, 2000 Maribor

Abstract
In contemporary education systems, the inclusion of environmental topics and sustainable development in curricula is crucial as it fosters awareness and responsibility towards the environment. The study focuses on analyzing the core objectives and subjects for pedagogical study programs at Slovenian universities. Environmental topics are mostly present within the content of specific subjects and are not integrated as key elements in educational process. The shortcomings are particularly evident in programs for primary education, where early environmental education is critical for developing students' awareness. The main findings highligjht the need for greater integration of environmental topics and sustainable development into pedagogical study programs to ensure that fure teachers acquire the appropriate knowledge and skills to teach those subjects. The research emphasizes the necessity of a systematic approach to including these topics to promote sustainable education at all levels.

Key words: environmental topics, pedagogical study programs, sustatainable development, teacher education, vertical integration.

Povzetek
V sodobnem izobraževalnem sistemu je ključnega pomena vključevanje okoljskih tematik in trajnostnega razvoja v učne programe, saj to omogoča razvoj ozaveščenosti in odgovornosti do okolja. Študija se osredotoča na analizo temeljnih ciljev in predmetnikov pedagoških študijskih programov slovenskih univerz, na podlagi analize temeljnih ciljev in predmetnikov programov, pri čemer ugotavlja, da so okoljske tematike večinoma prisotne le v okviru vsebin specifičnih predmetov in niso integrirane kot eden ključnih elementov izobraževalnega procesa. Pomanjkljivosti so zlasti opazne v programih za razredno stopnjo, kjer je zgodnje okoljsko izobraževanje ključnega pomena za razvoj ozaveščenosti učencev. Glavne ugotovitve kažejo na potrebo po večji integraciji okoljskih tematik in trajnostnega razvoja v pedagoške študijske programe, da bi bodoči učitelji pridobili ustrezna znanja in veščine za poučevanje teh tem. Raziskava poudarja nujnost sistematičnega pristopa k vključevanju teh vsebin za spodbujanje trajnostnega izobraževanja na vseh ravneh.

Ključne besede: izobraževanje učiteljev, okoljske tematike, pedagoški študijski programi, trajnostni razvoj, vertikalna povezanost.

1 INTRODUCTION

In recent years, we have witnessed major changes in industry and society [10]. New values, new ways of looking at the world and, consequently, new ways of teaching. The latter, along with learning, has undergone a transformation, as new forms of teaching and learning have emerged and teaching methods have also changed. In a context of societal change, where more and more emphasis is being placed on sustainability and environmentalism, the key question is how education adapts to this.

E-mail naslov/i: maja.krneza1@um.si (Maja Krneža), dejan.zemljak1@um.si (Dejan Zemljak)

Environmental education research has been a hot topic for several decades, as Hart and Nolan [6] have already pointed out a quarter of a century ago. They describe it as education that focuses in particular on topics that are directly and indirectly related to environmental issues. Concern for the environment has increased since then, as evidenced not only by the interest of researchers but also by the various strategies adopted. In Slovenia, a document with guidelines for sustainable development from pre-school to university education was drawn up in 2007, which defines the objectives and principles of education and training for sustainable development, as well as providing basic guidelines for such education at different levels [19].

UNESCO is also making similar efforts. A response to the challenges we face has been developed in the form of Education for Sustainable Development (ESD). They argue that limiting global warming requires tackling environmental, social and economic issues in an integrated way. Therefore, their document seeks the personal and social transformation needed to bring about the necessary change in society. UNESCO's efforts are essentially concerned with strengthening the capacity of governments to provide quality climate change education in the field of education, which includes the provision of technical support. In addition, it promotes innovative approaches and strengthens non-formal education through media, networking and partnerships. UNESCO is also working to strengthen students' knowledge, skills and values related to ESD by strengthening education for sustainable development. ESD also aims to strengthen the initiative to tackle interlinked global challenges such as climate change, biodiversity loss, unsustainable use of resources and inequality. The primary objective of ESD is to empower students of all ages to make informed choices, both individually and collectively, in environmental management [12].

The United Nations has also developed various initiatives to strengthen sustainability, such as the document defining the 17 Sustainable Development Goals (SDGs). While these do not directly relate to environmental education (EE), they do indicate which areas are important and which goals need to be achieved, and it is important to integrate them into the education process [17]. Similarly, environmental education is defined by the Berlin Declaration on Education for Sustainable Development as it emphasises EE in addressing global environmental challenges. The Declaration calls, among other things, for the integration of sustainable development into education worldwide. This is to promote the awareness, knowledge and action needed for a sustainable future. The Declaration also highlights the need for an integrated approach at all levels [15]. The European Commission has also provided basic guidance in this area. They call for the need to equip students with the knowledge, skills and attitudes needed to take action on sustainability. The proposal calls for ensuring access to high quality and inclusive education on climate change and sustainability for learners of all ages, for prioritising learning for environmental sustainability in education policies and programmes, for investing in green and sustainable equipment, for promoting support for sustainability at institutional level, and for mobilising national and European resources to invest in infrastructure, training, tools and resources to increase the resilience and readiness of education and training for a green transformation European Commission [3]).

This way of education engages learners to think differently about the environment and the situation in which they live. This, of course, should not neglect the learner's cognitive, emotional and social skills [2]. For the purpose of a more calibrated education in the field of environment and environment-related problems, the environmental education (EE) initiative has been developed. EE is a holistic process that enables people, especially students, to change their awareness of the environment and environmental problems. EE usually leads to the formation of a community that forms an awareness of the environment, which also leads to

more responsible environmental behaviour [9]. According to Oguz [9], it is about the education of individuals who acquire the following qualities, as illustrated in Figure 1.

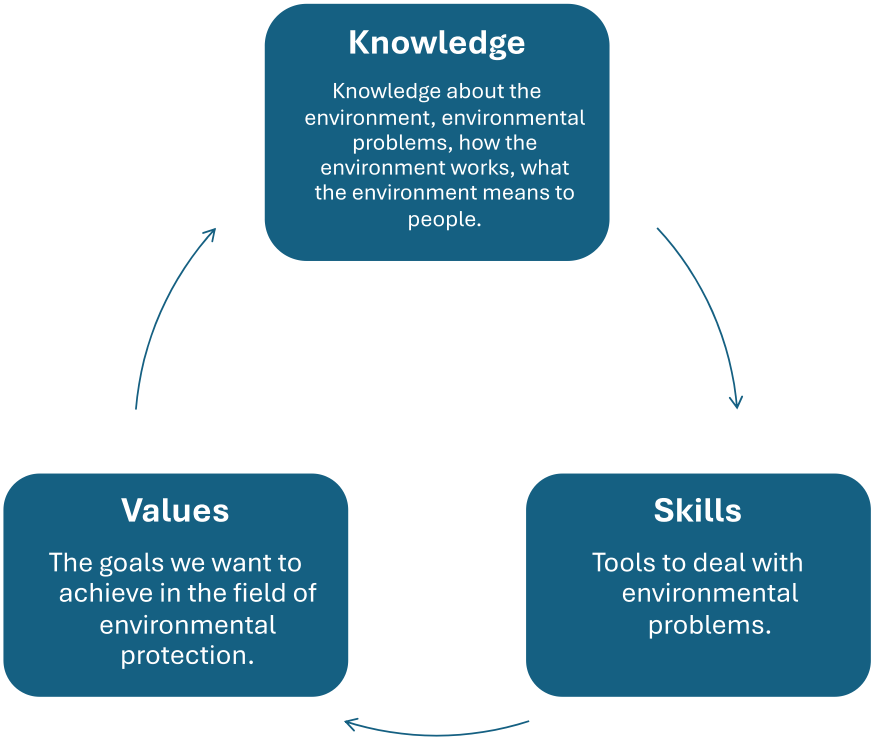


Figure 1: Knowledge, skills and values are inextricably linked in the EE process (adopted by Oguz [9]).

If an individual is to internalise positive attitudes towards the environment, which generally leads to positive behaviour in the environment, it is necessary that he or she receives appropriate education. Such education, as Altin et al. [1] state, is geared towards influencing the individual's behaviour in a way that can bring about change. Simply informing the individual about the content is not sufficient. Another important issue is the effectiveness of EE, which is only effective if it is based on life experience. It is therefore crucial to start the process of raising awareness and promoting sustainability at a young age, as this is when it is easiest to implement and more effective. The experience gained during education significantly shapes an individual's view of the world, including the environment in which they live. The transition from education to the working world requires special consideration. A "practice shock" is a possibility in the transition phase, when many beneficial effects of pre-service education are lost. However, a successful synthesis of theory and practice can occur if students are systematically introduced and supported with good mentoring in the transition from studies to life [22].

EE is most important in early childhood (especially in pre-school and the first years of education). It is during these ages that the foundations of personality are formed, which means that the child begins to separate from the environment. It is also at this time that emotional and value attitudes towards the environment, nature and people are formed. At the same time, it is important that the knowledge that students acquire is age-appropriate, as are the norms and rules of interaction with nature. Empathy for nature should not be neglected. EE thus not only helps to develop environmental awareness at an early age, but also fosters attitudes that define a sustainable and responsible lifestyle. The continuity and sustainability of EE is thus quite

important and has a long-term impact on children's moral and world-view behaviour. The period of primary education is an appropriate and favourable environment for children to develop a positive and sensible attitude towards the environment, to foster environmental awareness and to develop a sustainable lifestyle [8].

In universities and higher education institutions, EE is also often part of different study programmes. It can be presented as a stand-alone subject or as part of other courses. However, there is a significant difference here compared to lower levels of education, as students are already personality-formed and personality change is much more difficult than for younger students. Of course, it is extremely important to be aware that students who will soon enter the workplace and have a significant impact on various areas of society receive an education that enables them to develop positive attitudes towards the environment. It is therefore important that EE is not limited to theoretical knowledge but also includes practical experience. Such education influences individuals' behaviour by enabling them to relate theory to practical examples and real-life situations. Altin et al. [1] point out that education is only effective if it is based on life experiences, so it is important that students gain experience through various projects, research and field exercises that help them to form positive attitudes towards the environment. Students who have already developed positive attitudes towards the environment, either in their own lives or during their university education, can take this knowledge and experience forward into their professional work and personal lives. This is why we believe that EE is key to the development of environmentally aware and responsible individuals who will be able to contribute to solving environmental challenges in the future, even during their studies. Education based on life experience and practical examples enables students to develop lasting environmental values and to play an active role in preserving and improving the environment.

EE focuses primarily on environmental education and how to protect the environment, while ESD takes a broader approach, addressing not only environmental issues but also the social and economic dimensions of sustainability. It also focuses on the holistic development of individuals for sustainable living. EE is therefore a good example to include in the teaching of younger learners, as the focus of learning is on environmental protection, thus laying the foundations for further education on environmental sustainability. On the other hand, ESD is more appropriate for older children and young adults, including university students, as they are able to understand the wider links between the environment society and the economy. ESD thus prepares individuals to think and act in a holistic and sustainable way. In the case of teaching environmental topics at universities, ESD is therefore a more appropriate choice, as it offers students a holistic knowledge and provides a holistic understanding of the field [4], [21].

2 METHODOLOGY

Environmental issues and sustainable development are key in the modern education system to create responsible and aware individuals who understand the importance of nature protection and sustainable development. Based on an analysis of the curricula and their content in Slovenian primary schools and general grammar schools, it is clear that environmental topics are already an important part of the curriculum. The focus is on raising awareness and encouraging responsible behaviour towards the environment, enabling pupils to explore and understand the impact of human activities on the environment and the importance of sustainable development and conservation of natural resources [21]. Teachers play a key role in transferring environmental education knowledge to students. By understanding and being knowledgeable about environmental topics, they can effectively integrate environmental topics into their teaching and thus contribute to the development of environmental awareness among students.

This includes the ability to explain complex environmental issues and to promote critical thinking about the impact of human activities on the environment [21].

Research Objectives and Questions

The aim of this study is to explore how and to what extent environmental issues are included in the pedagogical curricula of Slovenian universities. The study focuses on the analysis of the integration of environmental topics in the study programmes and their content, and on how this affects the development of specific competences and skills of future teachers. Furthermore, it aims to explore the impact of the integration of environmental topics on the employability of graduates of these programmes. The study aims to identify the representation of environmental topics in the pedagogical study programmes, to examine the content of the environmental topics integrated, to assess the impact of environmental topics on the development of competences and to explore the impact of environmental topics on the employability of graduates.

In order to achieve the purpose and objectives of the thesis, we set out to answer the following fundamental research questions:

1. How are environmental issues represented in the core and general objectives of pedagogical study programmes at Slovenian universities?
2. How are environmental issues reflected in the curricula of pedagogical study programmes?
3. What impact does the inclusion of environmental topics have on the employability of graduates of pedagogical study programmes?

Eligibility Criteria and Information Sources

A review of the first- and second-level pedagogical degree programmes of three Slovenian universities, the University of Ljubljana, the University of Maribor and the University of Primorska, was carried out. The University of Ljubljana has a search engine on its website where a person with interest can search among study programmes for selected criteria, where we selected the Type of study programme (we were interested in Bachelor, Master and Single Master) in combination with the Study programme characteristic (Pedagogical). As it was possible to find in the search engine of study programmes of the University of Ljubljana, there are 0 Bachelor of Pedagogy study programmes, 14 Master of Pedagogy study programmes and 0 Single Master study programmes. The University of Maribor's search engine was also searchable using the built-in search engine. The search was carried out by KLASIUS-P-16 Educational Sciences and Teacher Education, which are separated by level according to colour and word information. The University of Maribor offers 4 first cycle university pedagogical degree programmes and 6 second cycle pedagogical degree programmes, with the second cycle Early Childhood Education programme not being included, as studies at the first cycle are conducted at the higher professional level. The University of Primorska's search engine allows searching for study programmes according to various criteria, among which we used the criteria of type of study (UNI and MAG) and KLASIUS-P-16 (01). There are 3 bachelor's degree programmes educating future teachers, while there are 9 corresponding master's degree programmes.

Searching Strategy and Selection Process

A review of the 1st and 2nd cycle teaching degree programmes was carried out. degree programmes of three Slovenian universities, the University of Ljubljana, the University of

Maribor and the University of Primorska, in terms of the basic data of the study programmes: the basic data of the study programme, the fundamental objectives of the programme, the general competences (learning outcomes), the subject-specific competences (learning outcomes), the conditions for admission, the selection criteria for admission limitation, the criteria for the recognition of skills acquired prior to enrolment in the programme, the assessment methods, the conditions for progression through the programme, the conditions for transfer between programmes, the conditions for completion of the programme, the conditions for completing individual parts of the programme, if included in the programme, and the subject list of the study programme. The information was retrieved from the faculties' websites, where it is available either in the form of links to the Proceedings or in the form of text published on the faculty's website.

Similar to the research conducted in Zemljak and Kerneža [21], all elements of the curriculum were searched for the keywords collected in Figure 2. The keywords presented in the scheme were selected based on a thorough review of relevant literature in environmental education, where these topics frequently emerge as central themes in curriculum development. The categorization into specific themes was informed by common groupings found in existing studies, providing a structured framework for analyzing their integration into educational programs. Two researchers conducted the search in alphabetical order - in all forms of the word. Once a keyword was found, a reading of the text referring to that keyword was carried out. All relevant parts of the text were transcribed and collected in a separate document. After collecting the data for each study programm, the contents were reviewed again. Than researchers compared the obtained results to identify differences and compared them with each other. The only notable distincsitons were in the phrasing used and the content of the same data, which remained the same. Every researcher went over and studied the final records again before creating their own study programm summaries for every study programm. The researchers then collaborated to analyze and evaluate these summaries, resulting in the final summary.

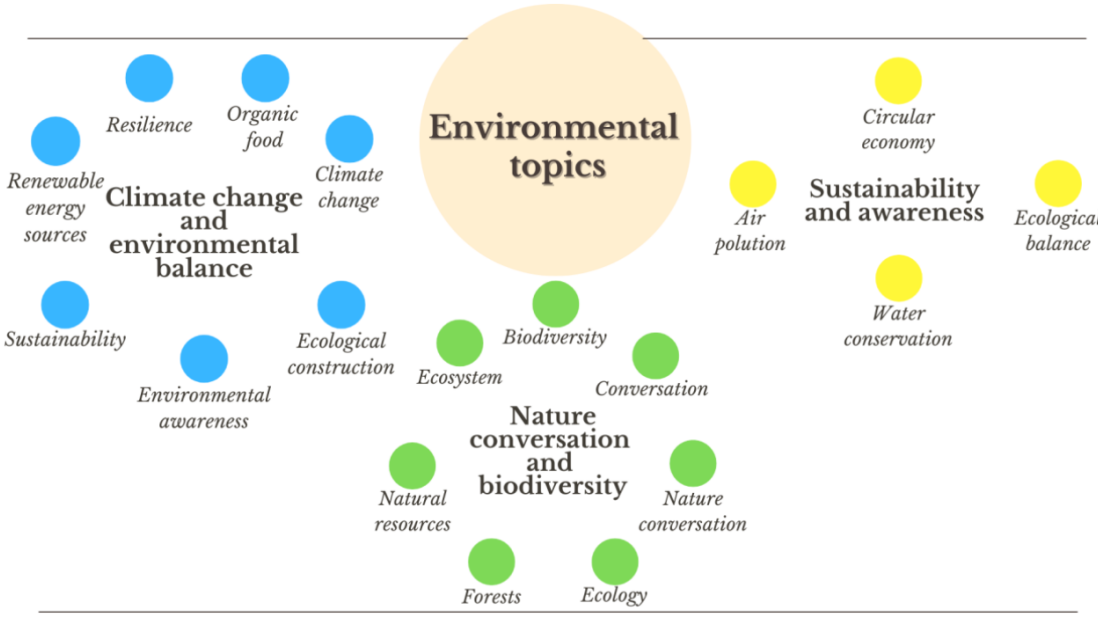


Figure 2: Concept of observed keywords [21]

3 ENVIRONMENTAL TOPICS IN SLOVENIAN UNIVERSITIES PEDAGOGICAL STUDY PROGRAMMS

In the interpretation of the collected data, universities, subjects and other details are not specifically mentioned, as the review focuses on a general analysis and assessment of the inclusion of environmental topics in the pedagogical study programmes at the Slovenian national level. However, some notable examples were identified during the review. For instance, natural science programmes observed to integrate environmental topics effectively across several courses, starting with basics and progressing to more advanced courses in the later years. This kind of vertical integration ensures that students build upon their knowledge progressively, enhancing their understanding and ability to teach these topics effectively. This approach allows for the identification of overarching trends and patterns that transcend individual institutional differences, avoids potential biases and ensures that the findings are applied to the whole field of education. By not anchoring the findings to specific institution programmes, the analysis seeks to provide insights that are relevant to the overall structure and strategy of teacher education in Slovenia. In this way, general trends and recommendations can be identified that are useful for improving the integration of environmental topics in the education of future teachers at national level, regardless of specific differences between the univerities or their programmes. While minor differences do exist between institutions, the findings overwhelmingly highlight common challenges and opportunities for improving environmental education across the board.

Representation of environmental issues in the core and general objectives of pedagogical study programmes at Slovenian universities

A review of pedagogical study programmes at Slovenian universities has shown that environmental issues are often under-represented in the core objectives of programmes. Most programmes do not include environmental objectives as (one of) the central elements of education, which indicates a lack of awareness of the importance of sustainable development in the context of teacher education. For example, in a thypical humanities programme, environmental topics were found only in elective cousres, with no clear link to core objectives, which could results in gradiates having limited exposure to these critical issues unless they avtively choose those electives. This is a significant gap, as the inclusion of envronmental objectives in core educational goals is critical for ensuring that sustianability becomes a fundamental aspect of future teachers' professional identity. Although environmental issues are in some cases included in broader themes or elective subjects, there is no systematic integration of the SDGs in the education of future teachers. This lack of integration can lead to fragmented and inconsistent exposure to environmental topics, which may not be sufficient to equip future educators with the necessary tools to address these issues comprehensively in their classrooms.

For example, one programme demonstrated effective vertical integration of envrionmental topics, beginning with course *Ecology*, which introduce students to fundamental ecological principles, including the relationship between organisms and their environment, as well as key concepts such as biodiversity, ecosystem services, and conservation. This foundational knowledge is then built upon in more advanced cousres, such as *Biological field practicum*, where students engage in hands-on learning experiences that involve assessing and analyzing real-world environmental issues. Finally, the programme includes capstone courses like *Biological research work*, where students conduct in-depth research on specific environmental challenges, applying the skills and knowledge acquired throughout their studies. This structured

progression from basic environmental concepts to practical applications ensures that students are well-prepared to teach these topics across different educational levels.

Science programmes tend to have better-defined environmental objectives, which include subjects such as ecology, nature conservation, and the sustainable use of natural resources. These programmes often provide a more structured approach to environmental education, ensuring that students receive a thorough grounding in key ecological princples and practices.

However, social sciences and humanities education programmes often lack specific objectives to promote environmental awareness. This means that graduates of these programmes may not acquire adequate knowledge and awareness of environmental issues, which reduces their ability to teach effectively in environmental topics. This discrepancy highlights a crucial need for curriculum reform in these fields to ensure that all future educators, regardless of their disciplinary focus, are equipped to contribute to the broader educational goal of fostering environmental literacy and sustainability. A deficiency in the fundamental objectives of education programmes may lead to a lower preparedness of future teachers to face the challenges related to sustainable development, which is crucial for the development of an informed and sustainable society.

A review of the general objectives and competences identified in the presentations of the pedagogical study programmes found that competences related to environmental issues are often addressed only indirectly or as part of broader objectives that are not specifically oriented towards sustainable development. Competences such as knowledge of the relationships between organisms and the environment and ethical principles of environmental protection appear more frequently in the natural sciences programmes, but are still under-emphasised. These programmes include topics such as sustainable use of natural resources and environmental protection, which contribute to the development of the basic skills and knowledge needed to understand complex environmental issues. However, even within these programmes, the depth and breadth of environmental education could be expanded to include more interdisciplinary approaches and practical applications, which are crucial for addressing the multifaceted nature of today's environmental challenges.

In contrast, competences related to environmental issues are rarely, if ever, identified or included in social sciences and humanities programmes. This means that graduates from these programmes may not acquire sufficient skills and knowledge needed to teach about environmental issues and sustainable development. The absence of these competences in concerning, as it suggests that a significant proportion of future educators may enter the workforce with limited understanding of how to integrate environmental sustainability into their teaching practices, which could perpetuate a gap in environmental education at the school level. The lack of such competences among teachers may have a negative impact on the education system, as students will not have the opportunity to acquire the knowledge and skills needed for responsible environmental management and sustainable development.

Reflecting environmental themes in the curricula of pedagogical study programmes

A review of the curricula of teacher education programmes showed that environmental topics are rarely included as a core part of the curriculum and are often limited to specific electives or specific fields of study. This reflects the lack of a comprehensive approach to integrating sustainability themes into teacher education. The sporadic inclusion of environmental topics in elective courses means that exposure to these critical issues is largely dependent on student choice rather than being guaranteed component of their education. The sporadic inclusion of

environmental topics in elective courses means that exposure to these critical issues is largely dependent on student choice rather than being a guaranteed component of their education.

For example, many study programmes only offer environmental topics within elective courses, meaning that students might complete their studies without ever encountering critical issues such as climate change or sustainable resource management if they do not select these electives. In science and technology programmes, environmental topics are part of the core curriculum, where subjects dealing with topics such as ecology, nature conservation and environmental ethics appear. These subjects allow students to develop a deeper understanding of environmental problems and acquire the practical skills needed to solve them. These programmes demonstrate the potential for effective integration of environmental themes when they are made a central component of the curriculum, offering a model that could be adapted by other disciplines.

However, in social sciences and humanities programmes, environmental topics are often limited to elective subjects that are not compulsory for more students. This limits opportunities to acquire comprehensive knowledge on environmental issues and sustainable development, which is crucial to prepare future teachers to teach these topics. The elective nature of these courses means that many students may graduate without ever engaging with crucial sustainability issues, leavin them less prepared to address these topics in their professional lives. The lack of compulsory courses related to environmental issues means that many graduates will not be exposed to the basic concepts of sustainable development and environmental protection, which may affect their ability to promote environmental awareness among students.

The impact of integrating environmental themes on the employability of graduates of teaching degree programmes

Based on a survey of teaching jobs in primary schools and general upper secondary schools as of 7 June 2024, 387 jobs were advertised on the Job Centre of the Republic of Slovenia, found with the keyword "teacher", with 185 primary school jobs and 32 upper secondary school jobs matching our interest. None of these jobs was found to specifically require knowledge of environmental issues. This lack of demand in job postings suggests that environmental competences are not currently prioritized in the hiring criteria for teaching positions, reflecting a broader systemic oversight of the importance of sustainability in education. Although knowledge of these topics may be important for teaching certain subjects, employers do not cite specific competences related to environmental topics as key to employability.

This suggests that the current labour market does not place a strong emphasis on environmental competences, but this does not diminish the importance of its integration into teaching programmes. Teachers with knowledge of environmental issues can make an important contribution to raising awareness and responsible environmental management among students, which is key to the sustainable development of society. Therefore it is crucial for educational institutions to proactively integrate environmental education into their curricula, recognizing that whil the immediate demand may be low, the long-term benefits of equipping teachers with these competences are significatn. This will contribute to creating a generation better prepared to address the complex challenges of the future.

5 CONCLUSION

Research has revealed that the integration of environmental topics into the pedagogical curricula of Slovenian universities is deficient, which may affect the preparation of future

teachers to teach these topics effectively [5], [14]. Despite some positive aspects, such as good vertical integration between subjects where environmental topics are more represented, there is still room for improvement [20]. Vertical integration is reflected in the transition of environmental topics from university curricula to primary and secondary school content, which allows for better continuity in the treatment of these topics across educational levels [13], [18].

An example of effective vertical integration can be seen in one of natural sciences programme, where environmental topics are systematically introduced at the foundational level through courses in ecology and environmental science. These subjects are followed by more advanced coureses, allowing students to build on their initial knowledge and explore more complex environmental issues as they progress through their studies. This progression ensures that students not only understand basic environmental principles but also learn to apply them in various contexts, preparing them to effectively teach these concepts at different educational levels.

It is worrying that environmental content rarely appears in the general objectives of study programmes and in the course syllabus, especially in the course syllabuses of the Classroom Education programme. This is critical, as it is classroom teachers who play a key role in the early formation of environmental awareness in students [11]. This reduces the opportunity for the integration of environmental topics in the early educational period, which may have an impact on students' overall awareness and responsibility towards the environment [7]. As some environmental topics may be addressed within general subjects and specific didactics, a more in-depth analysis would require a systematic review and evaluation of the curricula of individual subjects. This would allow for a more accurate assessment of how environmental topics are integrated into pedagogical study programmes and how well future teachers are prepared to teach these topics.

The findings highlight the need for educational institutions at national level to identify and integrate environmental issues as a core element of their curricula. This not only increases teachers' awareness and knowledge, but also contributes to the broader social change that is necessary to tackle contemporary environmental problems. In the further development of teacher education programmes, it is imperative that greater emphasis is placed on the integration of environmental issues and sustainable development as a central element of teacher education. This could increase teachers' willingness to teach these important topics, contributing to the creation of an informed and responsible society that is prepared to face contemporary environmental challenges [14]. It is important to develop a holistic approach that includes both theoretical and practical education, enabling teachers to integrate sustainable development into their teaching practice. In particular, there is a need to explore and develop methods to improve the integration of environmental topics into teaching programmes and to promote dialogue between educational institutions to achieve better integration of these topics.

Acknowledgement

This research was funded by Slovenian Research Agency (ARRS), grant number P5-0433; Digital Restructuring of Deficit Occupations for Society 5.0 (Industry 4.0).

Literature

[1] Altin, A., Teacher, S., Teacher, L., Altin, S. Kahraman, B. F. (2014). Environmental awareness level of secondary school students: A case study in Balıkesir (Türkiye). *Procedia - Social and Behavioral Sciences*, 141, 1208–1214. https://doi.org/10.1016/j.sbspro.2014.05.207

[2] Carleton-Hug, A., Hug, J. W. (2009). Challenges and opportunities for evaluating environmental education programs. *Evaluation and Program Planning, 33*(2), 159 –164.

[3] European Commission. (n. d.). *Learning for environmental sustainability.* Retrieved June 27, 2024, from https://education.ec.europa.eu/news/learning-for-environmental-sustainability

[4] Fang, W. T., Hassan, A. A., & LePage, B. A. (2023). *The living environmental education: Sound science toward a cleaner, safer, and healthier future*. Springer Nature.

[5] Goralnik, L., Dobson, T., & Nelson, M. P. (2014). Place-based care ethics: A field philosophy pedagogy. *The Canadian Journal of Environmental Education, 19*, 180–196.

[6] Hart, P. & Nolan, K. (1999). A critical Analysis of Research in environmental Education. *Studies in Science Education, 34*(1), 1–69.

[7] Kopina, H., & Meijers, F. (2014). Education for sustainable development (EDS): Exploring theoretical and practical challenges. *International Journal of Sustainability in Higher Education, 15*(2), 188–207. https://doi.org/10.1108/IJSHE-07-2012-0059

[8] Lamanauskas, V. (2023). The Importance of Environmental Education at an Early Age. *Journal of Baltic Science Education, 22*(4), 564–567. https://doi.org/10.33225/jbse/23.22.564

[9] Oguz, D. Çakci, I., & Kavas, S. (2010). Environmental awareness of University Students in Ankara, Turkey. *African Journal of Agricultural Research, 5*(19), 2629–2636

[10] Pereira, A. G., Lima, T. M., & Charrua-Santos, F. (2020). Industry 4.0 and Society 5.0: Opportunities and Threats. *International Journal of Recent Technology and Engineering, 8*(5), 3305–3308. https://doi.org/10.35940/ijrte.d8764.018520

[11] Summers, M., Corney, G., & Childs, A. (2004). Student teachers' conception of sustainable development: The starting-points of geographers and scientists. *Educational Research, 46*(2), 163–182. https://doi.org/10.1080/0013188042000222449

[12] UNESCO (2024). *What you need to know about education for sustainable development?* UNESCO. Retrieved June 27, 2024, from https://www.unesco.org/en/sustainable-development/education/need-know?hub=72522

[13] UNESCO. (2017). *Education for sustainable development goals: learning objectives*. UNESCO Publishing. https://doi.org/10.54675/CGBA9153

[14] UNESCO. (2018). *Issues and trends in education for sustainable development.* UNESCO Publishing.

[15] UNESCO. (2021). *Berlin Declaration on Education for Sustainable Development: Learn for our planet: Act for sustainability.* UNESCO. Retrieved from https://www.unesco.org/sites/default/files/medias/files/2021/05/Berlin-Declaration-on-ESD.pdf

[16] UNESCO. (2022). *Integration education for sustainable development (ESD) in teacher education in South-East Asia: A guide for teacher educators*. UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000265760.locale=en

[17] United Nations. (n. d.). *Sustainable development goals. United Nations.* Retrieved June 27, 2024, from https://www.un.org/sustainabledevelopment/sustainable-development-goals/

[18] Varela-Losada, M., Vega-Marcote, P., Perez-Rodriguez, U., & Alvarez-Lires, M. (2016). Going to action? A literature review on educational proposals in formal Environmental Education. Environmental *Education Research, 22*(3), 390–421. https://doi.org/10.1080/13504622.2015.1101751

[19] Vladna republika Slovenije. Ministrstvo za visoko šolstvo, znanost in tehnologijo. (2007). *Nacionalne smernice za razvoj informacijske družbe do leta 2010 [Government of the Republic of Slovenia. Ministry of Higher Education, Science and Technology. National Guidelines for the Development of the Information Society by 2010.]* https://www.gov.si/assets/ministrstva/MVI/SRI/nacionalne_smernice_VITR_2007.pdf

[20] Yaacob, A., & Abdullah, N. (2023). Environmental education for sustainable development (SD) among primary school teawchers. *Journal of Social Science, 9*(2), 35–42. https://doi.org/10.37134/ejoss.vol9.2.4.2023

[21] Zemljak, D., and Kerneža, M. (2023). Analysis of the inclusion of ecological topics in the curricula of Slovenian elementary and general grammar schools. *Dianoia, 7*, 51–69.

[22] Zuljan, M. V., & Požarnik, B. M. (2014). Induction and early‐career support of teachers in Europe. *European Journal of Education, 49*(2), 192–205. https://doi.org/10.1111/ejed.12080

VABILO AVTORJEM

Dianoia (grško διάνοια) po Platonu označuje védenje, razmišljanje o modelih stvarnosti, o naravoslovno-matematičnih in tehničnih temah. Uporabljajo ga matematiki (modeliranje) in znanstveniki (formuliranje problema), inženirji (načrtovanje sistema). Opredeljuje kompetenco, proces ali rezultat diskurzivnega razmišljanja, za razliko od neposrednega razumevanja obravnavane tematike. Aristotel to védenje naprej razdeli na teoretično (episteme) in praktično (phronesis).

Dianoia po Platonu torej označuje vmesni nivo človeškega spoznanja, prehod od intuitivnih občutkov do najglobljega spoznanja dejanskosti. Tako je idealna oznaka za objave v pričujoči reviji, ki povezujejo teoretična, znanstvena izhodišča z njihovo uporabno namembnostjo. Študentje, avtorji teh člankov, ste na prehodu od učenja k delu, od teoretičnega h konkretnemu, ki vas bo pripeljalo do kruha, do dela, s katerim boste odigrali svojo vlogo v družbi. Na tem prehodu pa poleg znanja, ki ga ponuja redno izobraževanje, potrebujete tudi izkušnje s konkretnih izzivov in mehke kompetence sodelovanja v ekipah delodajalcev, k čemur vas spodbuja in vam pri tem pomaga revija Dianoia.

V reviji bomo objavljali poljudne in strokovne članke s področja naravoslovja, matematike ali znanosti, ki uporabljajo znanja teh področij. Ciljna publika bralcev so v prvi vrsti delodajalci, ki tovrstna znanja potrebujejo in želijo izvedeti, kaj je kdo zanimivega razmislil na njihovem področju. V drugi vrsti so ciljna publika študentje, ki iščejo zamisli za svojo poklicno pot in lahko v reviji najdejo navdih za lastna raziskovanja in iskanje stikov s trgom dela.

Za kakovost izdelkov bo skrbel uredniški odbor in uredniški svet, v katerih so vrhunski strokovnjaki, povezani s področji, ki jih revija obravnava. Članki bodo anonimno recenzirani, o objavi pa na podlagi recenzije odloča uredniški odbor. Priporočljivo je, da avtorji besedilo spremenijo v skladu s priporočili recenzentov in da popravljeni članek z utemeljitvijo sprejema ali zavrnitve sprememb ponovno pošljejo v pregled. Uredništvo lahko objavo članka zavrne, če vsebinsko ali po merilih kakovosti ne ustreza standardom revije, o čemer avtorje obvestimo v najkrajšem možnem času.

S prispevkom v reviji bodo avtorji spodbujali širjenje znanja s področja naravoslovja in matematike ter tehnike oziroma izobraževanja teh področij in svoje poglede prenašali na trg dela in na prihajajoče generacije.

NAVODILA AVTORJEM

Avtorje prosimo, da pri pripravi članka upoštevajo naslednja navodila.

Če je članek napisan v slovenščini, naj ima angleški prevod naslova, povzetka in ključnih besed. Veseli bomo tudi prispevkov v angleščini, ki pa morajo imeti naslov, razširjen povzetek v obsegu 300 – 400 besed in ključne besede v slovenščini. Ključnih besed naj bo do šest.

Prispevki naj bodo zanimivi za širši krog bralcev. Ključna je intuitivna predstavitev zamisli in rezultatov, podrobnosti pa lahko ostanejo prihranjene za morebitni znanstveni članek, ki bi bil nadgradnja članka, objavljenega v reviji Dianoia.

Članek naj vsebuje naslov, ime avtorja (avtorjev) in sedež ustanove, kjer avtor(ji) dela(jo). Sledi naj povzetek, z največ 150 besedami, seznam ključnih besed in besedilo, ki ne presega 3000 besed. Besedilo naj bo zapisano v urejevalniku besedil MS Word 2010 oz. kasnejši ali LaTeX in naj uporablja objavljeno predlogo. Slike in tabele morajo biti oštevilčene in imeti natančen opis, da jih lahko razumemo brez preostalega besedila. Slike v elektronski obliki naj bodo visoke kakovosti v formatu PNG ali JPEG.

Prispevek v PDF obliki pošljite na naslov dianoia@um.si z zadevo: »Za revijo Dianoia«. Če bo sprejet v objavo, vas bomo prosili za izvorno obliko prispevka.