Rešavanje problema mrežnog koda upotrebom Grobnerovih baza

Dušan Orlović, Ivan Stanojević, Vojin Šenk

***Sadržaj* — U ovom radu je opisan postupak nalaženja mrežnog koda korišćenjem Grobnerovih baza. Prikazani su algoritmi koji daju odgovor na pitanje da li mreža ima linearno rešenje, zatim koje je polje sa najmanjim brojem elemenata nad kojim mreža ima linearno rešenje i na kraju, za dato konačno polje, koji je broj različitih linearnih rešenja. Svi ovi algoritmi koriste izračunavanje Grobnerovih baza za koje se zna da su eksponencijalne u vremenu u odnosu na broj promenljivih, stoga je veliki nedostatak ovih algoritama njihova kompleksnost.**

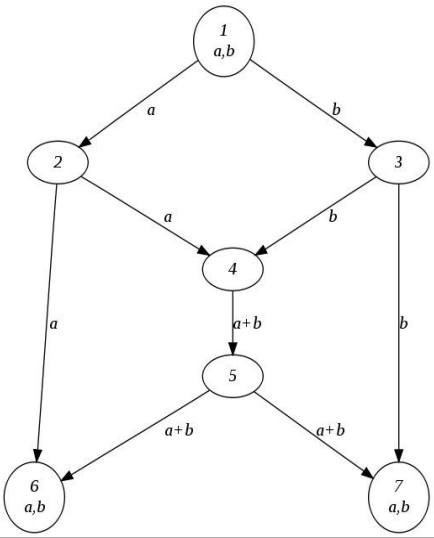
***Ključne reči* — grobnerove baze, mrežno kodovanje.**

I. UVOD

KORIST od mrežnog kodovanja uočena je još 2000. godine kada je dat najpoznatiji primer u kojem mrežni kod ima prednost u odnosu na klasično rutiranje [1], što je prikazano na sl. 1. Problem mrežnog koda je zadat na grafu (mreži) na kojem određeni čvorovi (izvori) šalju podatke i određeni čvorovi (odredišta) zahtevaju podatke. Podaci se biraju iz nekog konačnog skupa podataka koji ima strukturu polja. Na sl. 1. izvor je čvor *1* i šalje dva podatka a i b, a odredišta su čvorovi *6* i *7* koji zahtevaju podatke a i b. U nastavku se podrazumeva da je mreža sa usmerenim granama, jer kod mreža sa neusmerenim granama korist od mrežnog kodovanja nije toliko značajna [2]. Takođe važi da su grane jediničnog kapaciteta sa eventualnim paralelnim granama i da je mreža bez petlji (*directed acyclic network*).

Vidi se na sl. 1. da nije moguće klasičnim prosleđivanjem dostaviti oba podatka odredišnim čvorovima zbog uskog grla na grani *4-5*. Ukoliko se dozvoli da čvorovi vrše *linearnu kombinaciju* svojih ulaznih podataka (linearna kombinacija je sa koeficijentima iz istog polja iz kog su podaci) onda se zahtevi mogu ostvariti npr. ako čvor 4 šalje zbir $a+b$ onda odredišni čvorovi mogu odrediti podatak koji im nedostaje kao razliku svojih ulaznih podataka. Ako su sva odredišta zadovoljena tj. ako mogu da izračunaju zahtevane podatke na osnovu svojih ulaznih podataka i ako su korišćene samo linearne kombinacije u čvorovima onda mreža ima *linearno rešenje*. Uopšteno, ako su sva odredišta zadovoljena koristeći i eventualno nelinearne kombinacije, onda mreža ima (nelinearno) *rešenje*.

Dušan Orlović, Fakultet Tehničkih Nauka Novi Sad, orlovic@uns.ac.rs
Ivan Stanojević, Fakultet Tehničkih Nauka Novi Sad, cet_ivan@uns.ac.rs
Vojin Šenk, Fakultet Tehničkih Nauka Novi Sad, vojin_senk@uns.ac.rs



Sl. 1. Najpoznatiji primer mrežnog koda u kojem izvor *čvor 1* šalje dva podatka *a* i *b* ka odredišnim čvorovima *6* i *7*, a usko grlo na grani *4-5* čvor *4* rešava tako što šalje *zbir* svojih ulaznih podataka

Kada je u pitanju multikast mreža (jedan izvor šalje iste podatke ka više odredišta), kao što je na sl. 1, dokazano je [3] da ako mreža ima rešenje onda ima linearno rešenje i rešenje se može naći u polinomskom vremenu [4], [5]. U slučaju mreže sa više izvora, u [7] je dat primer mreže koja ima rešenje, ali nema linearno rešenje. Problemi koji se rešavaju u ovom radu su:

Problem 1: Za zadatu mrežu odrediti da li postoji konačno polje nad kojim mreža ima linearno rešenje.

Problem 2: Za zadatu mrežu koja ima linearno rešenje, odrediti konačno polje sa najmanjim brojem elemenata nad kojim mreža ima linearno rešenje.

Problem 3: Za zadatu mrežu i konačno polje nad kojim mreža ima linearno rešenje odrediti broj različitih rešenja.

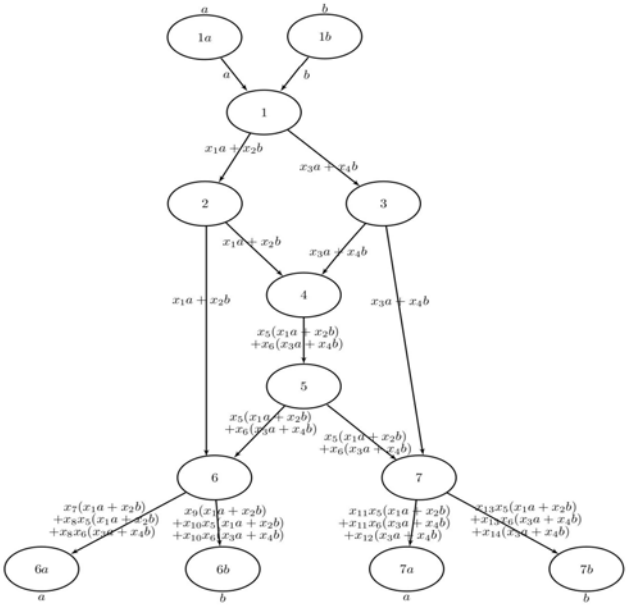
Svi ovi problemi pripadaju klasi NP teških problema [6]. Za rešavanje ovih problema u ovom radu je korišćena tehnika Grobnerovih baza (*Gröbner* ili *Groebner bases*), koja je opisana u drugom poglavlju. U trećem poglavlju su opisani algoritmi koji rešavaju zadate probleme, a u četvrtom poglavlju je dat zaključak. Za primer sa sl. 1 dat je odgovor na sva tri problema.

II. TEORIJSKA OSNOVA

A. *Algebarski pristup mrežnom kodovanju*

Svaki problem mrežnog koda (na acikličnoj mreži sa usmerenim granama) može da se predstavi pomoću sistema polinomskih jednačina, tako da taj sistem ima rešenje u nekom polju F ako i samo ako mreža ima linearno rešenje u polju F [8]. Drugim rečima, ova dva problema su ekvivalentna. Algoritam pomoću kojeg se dobija sistem jednačina je u jednostavan. Može da se pretpostavi da svaki izvor šalje jedan podatak i da svako odredište zahteva jedan podatak. U slučaju da izvor šalje više od jednog podatka, npr. k podataka, on se zamenjuje čvorom na koji je povezano k novih izvora koji šalju po jedan podatak. Slično, svako odredište koje zahteva više od jednog podatka, npr. n podataka, zamenjuje se čvorom na koji je povezano n novih odredišta koja zahtevaju jedan podatak. Ukoliko se jedan isti podatak šalje sa više izvora, onda se svi oni zamenjuju jednim izvorom. Opisane promene mreže sa sl. 1 prikazane su na sl. 2. Ako čvor ima jednu ulaznu granu, podatak na svakoj izlaznoj grani jednak je podatku na ulaznoj grani. Za svaki čvor koji ima više od jedne ulazne grane (na sl. 2 to su čvorovi *1,4, 6* i *7*) za svaki par ulazne i izlazne grane uvodi se jedna promenljiva koja predstavlja koeficijent u linearnoj kombinaciji pridruženoj toj izlaznoj grani. Na osnovu toga se na svakoj grani izračunava podatak koji se šalje. Na kraju se za svako odredište izjednačavaju koeficijenti uz podatak koji ono zahteva sa jedan, a uz podatak koji ono ne zahteva sa nula. Na taj način se dobija sistem jednačina (1), po dve za svako odredište *6a*, *6b*, *7a* i *7b*.

$$\begin{aligned}
x_1x_7 + x_1x_5x_8 + x_3x_6x_8 &= 1\\
x_2x_7 + x_2x_5x_8 + x_4x_6x_8 &= 0\\
x_1x_9 + x_1x_5x_{10} + x_3x_6x_{10} &= 0\\
x_2x_9 + x_2x_5x_{10} + x_4x_6x_{10} &= 1\\
x_1x_5x_{11} + x_3x_5x_{11} + x_3x_{12} &= 1\\
x_2x_5x_{11} + x_4x_6x_{11} + x_4x_{12} &= 0\\
x_1x_5x_{13} + x_3x_6x_{13} + x_3x_{14} &= 0\\
x_2x_5x_{13} + x_4x_6x_{13} + x_4x_{14} &= 1
\end{aligned} \qquad (1)$$



Sl. 2. Podaci na granama iz primera sa sl. 1

Dobijene jednačine su binarne (imaju samo koeficijente 0 i 1). Broj promenljivih je jednak zbiru proizvoda brojeva ulaznih i izlaznih grana svih čvorova sa više od jedne ulazne grane. Pojedinačan stepen svake promenljive je najviše jedan, a ukupan stepen nekog monoma (tj. broj promenljivih u jednom proizvodu) je manji od maksimalne dužine puta u granama od izvora do odredišta.

B. *Ideal polinoma sa koeficijentima iz konačnog polja*

U narednom izlaganju je sa R označen prsten, sa K polje, a sa F_q konačno polje sa q elemenata ($q = p^k$ gde je p prost broj). Neka je $R[x]$ skup svih polinoma sa koeficijentima iz R nad skupom promenljivih $x_1, x_2, ..., x_n$, koji se kraće označava sa x. *Ideal* I nad $R[x]$ je podskup $R[x]$ za koji važi da je zatvoren za sabiranje i spoljašnje-unutrašnje množenje, tj. ako $p \in I$ onda $pq \in I$ za sve $q \in R[x]$. Prema Hilbertovoj teoremi o bazama, svaki ideal I nad $R[x]$ ima konačan generatorski skup $\{p_1, \ldots, p_s\}$ (svaki polinom iz ideala jednak je linearnoj kombinaciji elemenata iz generatorskog skupa sa koeficijentima iz $R[x]$), što se označava sa $I = \langle p_1, \ldots, p_s \rangle$. *Skup nula* V *(varijetet, algebarski skup)* je podskup tačaka iz K^n za koji postoji skup polinoma koji se svi anuliraju na njima. *Ideal skupa nula* V je skup svih polinoma iz $K[x]$ koji se anuliraju na tom skupu nula V, $J(V) = \{p \in K[x] : p(u) = 0, u \in V\}$ (ovaj skup je ideal). *Nule ideala* I su skup svih tačaka iz K^n u kojima se svi polinomi iz tog ideala I anuliraju, $W(I) = \{x \in K^n : p(x) = 0, p \in I\}$. *Radikalni ideal ideala* I je skup $\sqrt{I} = \{p \in K[x] : \exists m \in \mathrm{N}, p^m \in I\}$ (ovaj skup je ideal). Ideal je radikalan ako važi $I = \sqrt{I}$. U opštem slučaju važi $V \subset W(J(V))$, a kako u konačnim poljima pomoću Lagranžove interpolacione formule za svaki skup tačaka $V \subset {F_q}^n$ mogu da se konstruišu polinomi koji se anuliraju samo na tom skupu onda za konačna polja važi formula $V = W(J(V))$ [9]. Za obrnut redosled W i J, za algebarski zatvorena polja K (svaki polinom nenultog stepena nad poljem K ima nulu iz tog polja K) važi teorema o nulama (Nullstellensatz) $\sqrt{I} = J(W(I))$ [11]. U konačnim poljima F_q ne važi da je ideal celog skupa tačaka prazan skup već je $J({F_q}^n) = \langle {x_1}^q - x_1, \ldots, {x_n}^q - x_n \rangle$ (kraće označeno sa $J({F_q}^n) = \langle x^q - x \rangle$) i za svaki ideal $I \subset F_q[x]$ važi da je ideal $I' = I + \langle x^q - x \rangle$ radikalan [10]. Skup nula ovih ideala je isti $W(I) = W(I')$ što daje teoremu o nulama za konačna polja u obliku

$J(W(I)) = I + \langle x^q - x \rangle$ [10]. Teorema o nulama ima svoju slabiju verziju da za ideal $I \subset K[x]$ gde je K algebarski zatvoreno polje važi da ideal I sadrži jedinicu ako i samo ako su nule ideala I prazan skup tj. $1 \in I \Leftrightarrow W(I) = \varnothing$ [11]. Verzija ove teoreme kada je K konačno polje glasi: skup polinoma $p_1, \ldots, p_m \in F_q[x]$ nema zajedničku nulu ako i samo ako $1 \in \langle p_1, \ldots, p_m, x_1^q - x_1, \ldots, x_n^q - x_n \rangle$ (to se vidi iz toga što ako ideal nema zajedničku nulu tj. $W(\langle p_1, \ldots, p_m \rangle) = \varnothing$, onda važi da je $J(W(\langle p_1, \ldots, p_m, x_1^q - x_1, \ldots, x_n^q - x_n \rangle)) = J(\varnothing)$, a na osnovu teoreme o nulama za konačna polja i na osnovu toga što polinom 1 nema nulu tj. $1 \in J(\varnothing)$ sledi $1 \in \langle p_1, \ldots, p_m, x_1^q - x_1, \ldots, x_n^q - x_n \rangle$, a obrnuto tvrđenje je očigledno). Još se može reći da polinomi iz nekog polja $p_1, \ldots p_m \in F_q[x]$ imaju zajedničku nulu u nekom proširenju polja $F_{q^i} \supset F_q, i \in \mathrm{N}$ ako i samo ako $1 \notin \langle p_1, \ldots, p_m \rangle$.

C. Grobnerove baze

Kod polinoma nad više promenljivih neophodno je da se definiše dobar redosled među monomima da se zna da li je npr. $x_1^3 x_2^5 > x_1^4$ i da važi da svaki strogo opadajući niz monoma konačan [11 s.53]. *Leksikografski redosled monoma* je redosled u kojem je $x_1^{\alpha_1} \cdots x_n^{\alpha_n} > x_1^{\beta_1} \cdots x_n^{\beta_n}$ ako je u vektoru razlike $(\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$ krajnji levi nenulti element pozitivan (na primer $x_1^3 x_2^5 < x_1^4$). *Graduisani leksikografski redosled* monoma se dobija kada se monomi prvo poređaju po ukupnom stepenu, a ako monomi imaju isti ukupan stepen onda važi leksikografski redosled (po ovom redosledu je $x_1^3 x_2^5 > x_1^4$). Na osnovu redosleda monoma za svaki polinom p možemo odrediti *vodeći monom* $LM(p)$ koji zajedno sa koeficijentom čini *vodeći član* $LT(p)$. *Algoritam redukcije polinoma* p *nad skupom polinoma* $\{p_1, \ldots, p_s\}$ je postupak u kojem se svaki član t polinoma p koji je deljiv nekim vodećim članom $LT(p_i),\ 1 \le i \le s$ (deljiv znači da može da se zapiše $t = l \cdot LT(p_i)$ za neki polinom l) zamenjuje odgovarajućim polinomom $\frac{t}{LM(p_i)}(LT(p_i) - p_i)$ čiji je vodeći monom po redosledu manji od t. Ovaj algoritam se završava u konačno mnogo koraka. Na kraju se dobija polinom kod kojeg ni jedan član nije deljiv sa vodećim članom bilo kog polinoma iz $\{p_1, \ldots, p_s\}$.

Grobnerova baza ideala I, $GB(I)$, je skup polinoma iz ideala $\{g_1, \ldots, g_s\}$ za koji važi da njihovi vodeći članovi generišu isti ideal kao i vodeći članovi polinoma iz I tj. $\langle LT(g_1), \ldots, LT(g_s) \rangle = \langle LT(I) \rangle$ gde je $LT(I)$ skup vodećih članova svih polinoma iz ideala I. S*-polinom* za polinome l i t se dobija tako što se skrate vodeći članovi

$$S(l,t) = \frac{LCM(LM(l), LM(t))}{LT(l)} l - \frac{LCM(LM(l), LM(t))}{LT(t)} t$$

gde je LCM najmanji zajednički sadržalac. Algoritam za dobijanje Grobnerove baze iz generatorskog skupa ideala je zasnovan na *Bukbergerovom kriterijumu,* koji kaže da je neki skup polinoma $\{p_1, \ldots, p_s\}$ Grobnerova baza ako i samo ako se S-polinomi [11] svih parova $p_i, p_j \in \{p_1, \ldots, p_s\}\ \ 1 \le i < j \le s$ redukuju na nulu nad tim skupom polinoma [11]. Bukbergerov algoritam jednostavno glasi: ako se za S-polinom nekog para polinoma iz generatorskog skupa dobije redukovan polinom koji nije nula onda se on dodaje u generatorski skup.

Standardni monomi ideala I, $SM(I)$, su monomi koji se ne nalaze u skupu vodećih monoma svih polinoma iz ideala $\{x^\alpha : x^\alpha \notin \langle LM(I) \rangle\}$ gde je $LM(I)$ skup vodećih monoma svih polinoma iz ideala. Skup standardnih monoma generiše vektorski prostor koji je izomorfan količničkom prstenu $K[x]/I$ (prsten polinoma u kojem su operacije sabiranja i množenja definisane isto kao i kod običnih polinoma s tim da se svaki polinom redukuje nad Grobnerovom bazom ideala I). Broj standardnih monoma $|SM(I)|$ može se lako dobiti iz Grobnerove baze, jer su to monomi koji nisu deljivi ni sa jednim vodećim monomom polinoma iz Grobnerove baze. Može se pokazati [10], [11 s.235] da je broj rešenja sistema jednačina nad konačnim poljem F_q jednak $|V(I)| = |SM(I + \langle x^q - x \rangle)|$, gde je I ideal koji generiše taj sistem jednačina.

D. Karakteristika sistema polinomskih jednačina

Kako je problem nalaženja mrežnog koda ekvivalentan rešavanju sistema polinomskih jednačina koje imaju samo koeficijente 0 i 1, onda skup polinoma u tim jednačinama, P, može da se posmatra kao skup polinoma sa celobrojnim koeficijentima, $P \subset \mathbf{Z}[x]$. Teorija Grobnerovih baza primenjena na takav sistem daje odgovor na pitanje nad kojim konačnim poljima sistem ima rešenje [12]. *Karakteristika konačnog polja* je prost broj r za koji važi da je $r = 0$ u tom polju. Za svako konačno polje $GF(p^k)$ karakteristika je prost broj p. *Skup karakteristika* polinomskog sistema jednačina $P \subset \mathbf{Z}[x]$ je skup karakteristika svih konačnih polja za koja sistem ima rešenje kada se posmatra u tom polju.

Skup karakteristika sistema je konačan ili komplementarno konačan (konačno mnogo prostih brojeva nisu u njemu) [12]. Definicija Grobnerove baze za polinome sa koeficijentima iz prstena je ista kao i kod polinoma sa koeficijentima iz polja. S obzirom da deljenje u prstenu u opšrem slučaju nije definisano, u algoritmu redukcije je deljivost nekog člana polinoma uslovljena i deljivošću njegovog koeficijenta. Takođe, u Bukbergerovom algoritmu prilikom izračunavanja S -polinoma moraju da se uzmu u obzir i vodeći koeficijenti. Ako Grobnerova baza $\{g_1,\ldots,g_s\}$ sistema $P \subset \mathbf{Z}[x]$ sadrži polinom jedan $g_i = 1$ za neko $1 \le i \le s$ onda sistem P nema rešenje posmatran u bilo kojem konačnom polju jer se jedinica uvek preslikava u jedinicu iz konačnog polja. Ako Grobnerova baza sistema $P \subset \mathbf{Z}[x]$ sadrži konstantan polinom veći od jedan $g_i = k, k > 1$ za neko $1 \le i \le s$ (ukoliko sadrži više takvih konstantnih polinoma onda se uzima njihov najveći zajednički delilac jer ih on sve generiše), onda će sistem P imati rešenja u konačnim poljima čija karakteristika deli k jer će u tim poljima važiti $k = 0$, a ideal sistema posmatranog u tim poljima neće sadržati jedinicu pa sistem ima rešenje u nekom od proširenja osnovnog polja [12]. Konačno, u slučaju da Grobnerova baza ne sadrži ni jedan konstantni polinom, onda je skup karakteristika sistema komplementarno konačan, tj. skup svih prostih brojeva bez tzv. loših karakteristika. Neka je s najveći zajednički delilac vodećih koeficijenata polinoma iz Grobnerove baze, a S skup njegovih prostih faktora. Neka je G' Grobnerova baza dobijena dodavanjem s u polaznu bazu i sprovođenjem Bukbergerovog algoritma i neka je T skup prostih faktora konstantnog polinoma u G'. Tada je skup loših karakteristika $S \setminus T$ [12].

III. Algoritmi

Iz predhodne teorijske osnove lako se izvode algoritmi za rešavanje problema koji su postavljeni na početku. Prvi problem je da se za zadatu mrežu odredi da li postoji konačno polje nad kojim postoji linearno rešenje i odgovor je da postoji ako i samo ako Grobnerova baza sistema $P \subset \mathbf{Z}[x]$ ne sadrži jedinicu. Drugi problem je da se odredi najmanje polje nad kojim mreža ima linearno rešenje i algoritam je da se pretraživanjem skupa karakteristika sistema $\{r_1, r_2, \ldots\}$ nađe najmanje polje tako što se započne od najmanje karakteristike r_1 i sukcesivnim proširivanjem osnovnog polja $GF(r_1^j)$, $j = 1,2,3,\ldots$ posmatra Grobnerova baza ideala $\left\langle p_1,\ldots,p_m, x_1^{r_1^j} - x_1,\ldots,x_n^{r_1^j} - x_n \right\rangle$. Ukoliko se prilikom računanja dobije polinom jedan (što znači da u tom polju ne postoji rešenje) nastavlja se sa daljim proširivanjem. Proširivanje se prekida kada se dobije da Grobnerova baza ne sadrži polinom jedan (što znači da za to polje npr. $GF(r_1^k)$ postoji rešenje). Isti postupak se ponavlja i za ostale karakteristike $r_i > r_1$ i njihova proširenja sve dok je veličina polja manja od do tada najmanjeg polja za koje postoji rešenje. Rešenje trećeg problema, da se za zadato polje izračuna broj različitih rešenja, dobija se uz pomoć formule $|V(I)| = |SM(I + \langle x^q - x \rangle)|$. Za primer sa sl. 1. dobija se da je skup karakteristika ceo skup prostih brojeva, da je najmanje polje veličine 2 i da je za to polje broj standardnih monoma 6, $\{1, x_{11}, x_{12}, x_{12} \cdot x_{13}, x_{13}, x_{14}\}$, stoga postoji 6 rešenja. Prikaz rešavanja ovog i drugih primera mrežnog koda uz pomoć Sage programa može se videti putem interneta [13].

IV. Zaključak

U ovom radu je prikazan način rešavanja problema u mrežnom kodovanju koji su NP-teški, zbog čega algoritmi rade samo za male mreže (koje generišu do 15 promenljivih). Stoga je dalji rad usmeren u nalaženju efikasnijih postupaka i paralelizaciji datih algoritama.

Literatura

[1] Ahlswede, Cai, Li, Yeung, Network Information Flow, IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204-1216, July 2000.

[2] Baochun Lin, Microsoft research speaker at www.ResearchChannel.org, How helpful is Network Coding, 2006.

[3] Li, Yeung, Chai, Linear network coding, IEEE Trans. Inf. Theory, vol. 49, no. 2, pp. 371-381, Feb. 2003.

[4] S. Jaggi, P. Sanders, P.A. Chou, M. Effros, S. Egner, K. Jain, L.M.G.M Tolhuizen, Polynomial time algorithms for multicast network code construction, IEEE Trans. Inform. Theory, vol. 51, no. 6, pp. 1973-1982, June 2005.

[5] Dusan Orlovic, Implementation of Polynomial Time Algorithms for Network Coding – with Python language, Telfor 2008.

[6] April Rasala Lehman, Eric Lehman, Complexity Classification of Network Information Flow problems, SODA '04: Proc: 15th Annu. ACM-SIAM Symp. Discrete algorithms, New Orleans, LA 2004 pp. 142-150.

[7] Randall Dougherty, Christopher Freiling, Kenneth Zeger, Insufficitency of Linear Coding in Network Information Flow, IEEE Trans. On Inf. Theory, vol. 51, no. 8, August 2005

[8] Randall Dougherty, Cris Freiling, Kenneth Zeger, Linear Network Codes and System of Polynomial Equations, IEEE Trans. On Inf. Theory, vol. 54, no. 5, May 2008

[9] R. Germundsson, Basic Results on Ideals and Varieties in Finite Fields. 1991 http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.54.937

[10] Sicun Gao, Counting Zeros over Finite Fields with Groebner Bases, www.andrew.cmu.edu/user/avigad/Students/gao_ms_thesis.pdf '09

[11] David Cox, John Little, Don O'Shea, Ideals, Varieties and Algorithms, Third edition, Springer 2007

[12] Rosemary Baines, Peter Vamos, An algorithm to compute the set of characteristics of a system of polynomial equations over the integers, Journal of Symbolic Computation 2003

[13] SageMath NoteBook http://demo.sagenb.org/home/pub/44/

Abstract

This paper describes the algorithms for finding the network code solution. The algorithms presented here answer the question of whether the network has a linear solution, which is a the smallest field over which the network has a linear solution and for a given finite field, what the number of different linear solutions is.

Network coding using Grobner bases

Dušan Orlović, Ivan Stanojević, Vojin Šenk