Математички факултет
Универзитета у Београду

МОЛБА
ЗА ОДОБРАВАЊЕ ТЕМЕ МАСТЕР РАДА

Молим да ми се одобри израда мастер рада под насловом:

Велики лов на триноме

Значај теме и области:
Несводљив полином $f(x)$ степена n над коначним пољем $GF(2)$ је примитиван ако је најмање k за које $f(x)$ дели $x^{2^k-1}-1$ једнако n. Ако је n прост број, онда је сваки несводљив полином степена n примитиван. "Велики лов на триноме" (The Great Trinomial Hunt [1]) је пројекат чији је циљ проналажење тринома $1+x^k+x^n$ великог простог степена n. Мотив је једноставан: ако је трином $1+x^k+x^n$ примитиван, онда бинарни рекурентни низ $x_N = x_{N-k}+x_{N-n} \pmod 2$, $N = n+1, n+2, \ldots$ за произвољних првих n чланова има период дужине 2^n-1 и јако добре статистичке особине, па се може користити као основа за генераторе псеудослучајних бројева. За степене тринома узимају се Мерсенови прости бројеви (прости бројеви облика 2^p-1, где је p прост број), чијим се проналажењем бави други велики пројекат GIMPS (Great Internet Mersenne Prime Search). На пример, $7 = 2^3-1$ је Мерсенов број, полином $1+x+x^7$ је примитиван, а низ $x_N = x_{N-1}+x_{N-7} \pmod 2$ има период дужине $2^7-1 = 127$. Провера да ли је трином $1+x^k+x^n$ несводљив своди се проверу да ли је узајамно прост са полиномима $x^{2^i-1}-1$, $i = 1,2,\ldots,n-1$. Алгоритам је једноставан, али не ако је нпр. $n = 2^{82589933}-1$, Мерсенов број откривен у јуну 2021. године. У раду [1] описано је неколико поступака за убрзавање основног теста несводљивости тринома.
Специфични циљ рада:
Циљ рада је описати и реализовати алгоритме за тестирање несводљивости бинарних тринома из рада [1], упоредити ефикасност реализованих програма и програма који се могу наћи на сајту посвећеном лову на триноме. Реализованим програмом треба пронаћи (већ пронађени) трином што већег степена.

Остале битне информације:
Литература:
[1] R. P. Brent, P. Zimmermann, The Great Trinomial Hunt, Notices of the American Mathematical Society, 58(2) (2011), 233–239

Јована Павловић, 1065/2020 МР Сагласан ментор Миодраг Живковић

(име и презиме студ., бр. инд., ознака програма и модула)

_____
(својеручни потпис студента)

_____
(датум подношења молбе)

_____
(својеручни потпис ментора)

Чланови комисије

1. др Весна Маринковић, ванр. проф.
2. др Стефан Мишковић, доцент

Катедра за рачунарство и информатику је сагласна са предложеном темом.

_____ _____

(*шеф катедре*) (*датум одобравања молбе*)