Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales

Ref. Expte. Nº 789/2021

Ciudad Autónoma de Buenos Aires, 31 de mayo de 2021

VISTO:

La nota presentada por la Dirección del Departamento de Computación, mediante la cual eleva la información del curso de posgrado **Curso intensivo en generadores cuánticos de números aleatorios** para el año 2021,

CONSIDERANDO:

lo actuado por la Comisión de Doctorado,
lo actuado por la Comisión de Posgrado,
lo actuado por este Cuerpo en la sesión realizada en el día de la fecha,
en uso de las atribuciones que le confiere el Artículo 113º del Estatuto Universitario,

EL CONSEJO DIRECTIVO DE LA FACULTAD
DE CIENCIAS EXACTAS Y NATURALES
R E S U E L V E:

ARTÍCULO 1º: Aprobar el nuevo curso de posgrado **Curso intensivo en generadores cuánticos de números aleatorios** de 15 horas de duración, que será dictado por el Dr. Gabriel Senno con la colaboración del Dr. Alejandro Díaz-Caro.

ARTÍCULO 2°: Aprobar el programa del curso de posgrado **Curso intensivo en generadores cuánticos de números aleatorios** para su dictado en julio de 2021.

ARTÍCULO 3°: Aprobar un puntaje máximo de medio (0,5) punto para la Carrera del Doctorado.

ARTÍCULO 4°: Disponer que de no mediar modificaciones en el programa, la carga horaria y el arancel, el presente Curso de Posgrado tendrá una vigencia de cinco (5) años a partir de la fecha de la presente Resolución.

ARTÍCULO 5º: Comuníquese a todos los Departamentos Docentes, a la Dirección de Estudiantes y Graduados, a la Biblioteca de la FCEyN y a la Secretaría de Posgrado con copia del programa incluida. Cumplido, archívese.

RESOLUCIÓN CD Nº 0752

Dr. PABLO J. GROISMAN
Secretario Adjunto de Posgrado
FCEyN - UBA

Dr. JUAN CARLOS REBOREDA
DECANO

Formulario para la presentación de Cursos de Posgrado/Doctorado – Res. CD2819/18 - ANEXO 1

Informaciónacadémica

Añodepresentación(*)
2021

1-a-

Departamentodocentequeiniciaeltrámite:
Computación
Nombredelcurso:
Cursointensivoengeneradorescuánticosdenúmerosaleatorios
Nombre,CargoyTítulodeldocenteresponsable:
GabrielSenno,Profesorvisitante,DoctorenCienciasdelaComputacióndelaUniversidaddeBuenosAires.
Encasodedictarseenparaleloconunamateriadegrado,nombredelamisma:
Generadorescuánticosdenúmerosaleatorios
NombreyTítulodelos docentesquecolaborancon eldictadodelcurso(*) (*):
AlejandroDíaz-Caro.DoctorenComputacióndelaUniversitédeGrenoble
Fechapropuestaparaelprimerdictadoluegodelaaprobación:
Julio 2021 (ECI2021)

Duración:	
Duracióntotalenhoras	15
Duraciónensemanas	1

Distribucióncargahoraria:

Númerodehorasdeclasesteóricas	10
Númerodehorasdeclasesdeproblemas	5
Númerodehorasdetrabajosdelaboratorio	
Númerodehorasdetrabajodecampo	
Númerodehorasdeseminarios	

Formadeevaluación:
Examenindividualdomiciliario.
Lugarpropuestoparaeldictado(departamento,laboratorio,campo,etc.):
Modalidad virtual

Puntaje propuesto para la carrera de doctorado: 0.5 puntos

Númerodealumnos:	Mínimo: 5	Máximo:50
Audienciaaquién estádirigido elcurso:		
EstudiantesdedoctoradoenCs.delaComputaciónyespecialidadesafines.		

Necesidadesmaterialesdel curso:
Saladereunionesvirtual.

1-b-

Programaanalíticodelcursoconbibliografía(puedeadjuntarseenhojasseparadas):
La capacidad de generar números aleatorios es un recurso fundamental en informática, conimportantesaplicacionesensimulaciónnuméricayencriptografía.Elcarácterinherentementealeatorio delamecánica cuánticaconviertea lossistemascuánticos enfuentesideales de entropía. Enlosúltimosaños,estehechohaimpulsadoeldesarrollocomercialdegeneradorescuánticosdenúmeros aleatorios(QRNG,porsussiglaseninglés)conbitestescercanosasucontraparte basada en la (sólo) aparente aleatoriedad de ciertos sistemas clásicos (p. ej. caóticos). Más aún, elcarácternolocaldelascorrelacionesentresistemascuánticos entrelazadospermiteeldiseñodeQRNGs “independientes del dispositivo” (DI-QRNGs, por sus siglas en inglés) cuya salida se puedecertificarimpredecibleaúnparaunespíaquehayapodidoalterareldispositivodemanera maliciosa. En este curso estudiaremos los distintos protocolos para la generación cuántica de númerosaleatorios,yendodesdeelesquemabásicodetrásdelosQRNGshoydisponiblesenlaindustriaal ateoríade DI-QRNG.Porúltimo, discutiremosesquemassemi-DI que,acambio derelajar levementelasgarantíasdeseguridadqueseobtienenconelesquemaDI,permitenimplementa ciones más cercanas alas capacidades tecnológicas actuales. **Programadelcurso**: ● Extractoresdealeatoriedad ● Generadorescuánticosdenúmerosaleatorios(QRNG) ● No-localidad de Bell ● Generacióndealeatoriedadprivadaenelesquema“independientedeldispositivo”(DI-QRNG) ● Unbalanceentregarantíasteóricasyfacilidaddeimplementación:elesquemasemi-DI Programadetalladopordía: ● Lunes o Introducciónalproblemadelageneracióndenúmerosaleatorios o Entropía,entropía-mínimayfuentesdébilesdeentropía o Extracciónde aleatoriedad ● Martes o Breveintroducciónalformalismocuántico. o Primerageneracióndegeneradorescuánticosdenúmerosaleatorios ● Miércoles o Generacióndealeatoriedadenunesquemacriptográfico(aleatoriedadprivada) o No-localidaddeBellyelesquema“independientedeldispositivo”(DI)

- Jueves
  - Amplificaciónyexpansióndealeatoriedadprivadaenelesquema DI
  - Adversariocuánticovs.adversarioclásico
  - LahipótesisIID(experimentosindependienteseidénticamentedistribuidos)
- Viernes
  - Elesquemasemi-DIparageneracióndealeatoriedadprivada
  - Generacióndealeatoriedadprivadaconunahipótesissobrelaenergíamediadelossistemascuánticos

Bibliografía:

- Arora,S.,&Barak,B. (2009).Computationalcomplexity:amodernapproach.CambridgeUniversityPress, chap. 21.
- Herrero-Collantes,M.,&Garcia-Escartin,J.C. (2017).Quantumrandomnumbergenerators.Reviews of ModernPhysics, 89(1), 015004.
- Brunner,N.,Cavalcanti,D.,Pironio,S.,Scarani,V.,&Wehner,S.(2014).Bellnonlocality.Reviews of Modern Physics, 86(2), 419.
- Acín,A.,&Masanes,L. (2016).Certifiedrandomnessinquantumphysics.Nature,540(7632),213-219

BibliografíaAdicional:

- Nielsen,M.A.,&Chuang,I.L.Quantum ComputationandQuantumInformation.Cambridge University Press, 2010. Capítulos2, 9 y 11.
- Scarani,V.Bellnonlocality.OxfordUniversityPress,2019.Capítulos2,3y8
- Arnon-Friedman,R.Device-IndependentQuantumInformationProcessing:ASimplifiedAnalysis.Springer Nature, 2020. Capítulos 7 y 9.
- Arora,S.,&Barak,B.Computationalcomplexity:amodernapproach.CambridgeUniversity Press, 2019. Capítulo 21.

1-c-

Actividadesprácticaspropuestas(puedeadjuntarseenhojasseparadas):

(*)Todosloscursostendránunavalidezde5años

(*)(*)Lasactualizacionesdelosdocentescolaboradoressoninformadosporla Direcciódepartamentalalinicio de cadadictadodelcurso

Firma Subcomisión Doctorado

Firma del docente responsable

E-mailyteléfonodeldocenteresponsable

gsenno@gmail.com
+34 622346833
adiazcaro@icc.fcen.uba.ar
011 15 2889 1452

Formulario para la presentación de Cursos de Posgrado/Doctorado - Res. CD2819/18 - ANEXO 2

SolicituddeFinanciación

Añodepresentación(*)
2021

Departamentodocentequeiniciaeltrámite:
Nombredelcurso:
NombreyTítulodeldocenteresponsable:

Costopropuestodelcursoporalumno(*):

Justificacióndelmontopropuesto:

(*)Lasexcepcionesaplicablesparacadaalumnoserán consistentesconlareglamentacióndelConsejoDirectivoque regulalosaranceles yexcepciones(ResCD484/13).Eldocenteresponsabledel curso solicitarálasexcepcionespornotaalconsejodirectivoatravésdeMesadeEntradas.