CURRICULUM VITAE

Alberto Zanoni

ANAGRAFE Nato il 14/3/1969.

CITTADINANZA Italiana.

TITOLI

1. Laurea in Scienze dell'Informazione - Università di Pisa, 16/6/1993 (esame sostenuto in data 11/6/1993) : 110/110 e lode.
2. Laurea in Matematica - Università di Pisa, 7/5/1996 (esame sostenuto in data 29/4/1996) : 107/110.
3. Dottorato di Ricerca in Matematica - Università degli Studi di Firenze, XIV ciclo (1998-2002), A.A. 2001 - 2002, 11/3/2003.

SERVIZIO MILITARE Ufficiale di Complemento (Sottotenente) del Corpo Automobilistico presso la Scuola Trasporti e Materiali in Cecchignola - Roma (7/1993 - 10/1994). Insegnamento scuola guida (patente C) e fisica. Avanzamento al grado di Tenente (1999).

PASSATO E PRESENTE

- Membro del team di Pisa del progetto FRISCO (contratto di ricerca) : 5/1996 - 12/1998.
- Esercitatore di Matematica Discreta per il corso di laurea in Informatica presso l'Università di Pisa (A.A. 1996–97, 1997–98, 1998–99).
- Borsista (Algebra computazionale) presso il dipartimento di Matematica, Università di Pisa (3/2003 - 3/2005).
- Collaboratore FILAS: ricerche in ambito algebrico/crittografico (10/10/2005 - 10/10/2006, 17/4/2007 - 16/10/2008)
- Assegnista/borsista presso il centro Vito Volterra, Università "Tor Vergata", Roma (1/10/2006 - 16/4/2007, 1/4/2010 - 31/8/2010)
- Assegnista presso il Dipartimento di Scienze Statistiche, Università "Sapienza", Roma (1/3/2011 - 28/2/2013)
- Assegnista presso il Dipartimento di Scienze Statistiche, Università "Sapienza", Roma (1/10/2015 - oggi)

SCUOLE / CORSI ESTIVI

- Seminario a numero chiuso organizzato da IBM "Tecnologie dell'informazione: prospettive scientifiche e culturali" - Spoleto (PG), 9/1992.
- Corso estivo di Ricerca Operativa organizzato da S.M.I. - Cortona (AR), 8/1996.
- "XIII Cursos de Verano" - Laredo (Spagna), 9/1997.
- Diffiety School - (I) Forino (AV), 7/1998. (II) Petruro (AV), 2-3/1999. (III) Pereslavl-Zalessky (Russia), 8/1999.
- Corso estivo di fisica matematica, organizzato da C.I.M.E. - Cetraro (CS), 9/1999.
- Corso estivo di algebra organizzato da S.M.I. - Cortona (AR), 7/2000.
- Corso estivo di geometria non commutativa organizzato da C.I.M.E. - Martina Franca (TA), 9/2000.

CONFERENZE, WORKSHOP, CONGRESSI, ESPERIENZE ALL'ESTERO

FRISCO Open Workshop : INRIA, Sophia Antipolis, Nizza (Francia), 18-20/3/1997.
4^{th} International Conference ACA : Praga (Repubblica Ceca), 8/1998.
Workshop on systems of algebraic/differential equations : Karlsruhe (Germania), 18-19/3/2002.
8^{th} Rhine workshop on Computer Algebra : Mannheim (Germania), 21-22/3/2002.
Conferenza "Applications of Commutative Algebra" : Catania, 3-6/4/2002.
Workshop "Real algebraic and analytic geometry" : Santander (Spagna), 13-15/6/2002.
8^{th} International Conference ACA : Volos (Grecia) 25-28/6/2002.
18^{th} IFIP World Computer Congress : Tolosa (Francia), 22-27/8/2004.
6^{th} International Symposium SYNASC04 : Timişoara (Romania), 26-30/9/2004.
8^{th} International Workshop CASC 2005 : Kalamata (Grecia), 12-16/9/2005.
Workshop on Approximate Commutative Algebra : Linz (Austria), 20-24/2/2006.
Workshop on Gröbner Bases in Cryptography, Coding Theory, and Combinatorics : Linz (Austria) 1-6/5/2006.
9^{th} International Workshop CASC 2006 : Chişinau (Moldova), 11-15/9/2006.
Workshop on Information & Communication Technology : Sendai (Giappone), 21-23/12/2006 - Invited speaker
International Symposium ISSAC 2007 : Waterloo (Canada), 29/7-1/8/2007.
International Conference ICTAMI 2009 : Alba Iulia (Romania), 3-6/9/2009
11^{th} International Symposium SYNASC09 : Timişoara (Romania), 26-29/9/2009
International Symposium ISSAC 2010 : Monaco (Germania), 25-28/7/2010.
International Conference ICTAMI 2011 : Alba Iulia (Romania), 21-24/7/2011
13^{th} International Symposium SYNASC11 : Timişoara (Romania), 26-29/9/2011
14^{th} International Workshop CASC 2012 : Maribor (Slovenia), 3-6/9/2012.

- Ricerca di algebra computazionale a Santander (Spagna), Universidad de Cantabria: 13/1 - 8/2/2003 e 11/5 - 6/6/2003.
- Presentazione seminario su un approccio algebrico polinomiale ad AES: Università di Cork (Irlanda), 11/2004.
- Corso di algebra computazionale di base presso la Tokyo University of Science (Noda, Giappone), 3/2006

PUBBLICAZIONI

⋆ *Gröbner Bases Specialization through Hilbert Functions: The Homogeneous Case* - SIGSAM BULLETIN, Communications in Computer Algebra. Volume 34, N.1, Marzo 2000, issue 131. ACM Press, USA, pp 1 - 8. (con M-J Gonzalez-Lopez, L. Gonzalez-Vega, C. Traverso).

⋆ *Numerical stability in Gröbner Basis Computation* - Proceedings of the 8^{th} Rhine Workshop on Computer Algebra. H. Kredel, W. K. Seidler, ed. - Mannheim, Marzo 2002. pp. 207 - 216

⋆ *Numerical Stability and Stabilization of Groebner Basis Computation* - Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, Université de Lille, France, ACM press, New York, USA, Teo Mora ed. - 7/2002. (con C. Traverso)

⋆ *An Algebraic Interpretation of AES-128.* Advanced Encryption Standard - AES: 4th International Conference. Bonn, Germania, Maggio 2004. H. Dobbertin, V. Rijmen, A. Sowa ed. Lecture Notes in Computer Science, volume 3373/2005. Springer-Verlag ed. ISBN: 3-540-26557-0 p.84 - 97 (con I. Toli)

⋆ *Looking inside AES and BES* in Exploring new frontiers of Theoretical Informatics Proceedings of the 18th IFIP World Computer Congress - TC1 3rd International Conference on Theoretical Computer Science (TCS2004) 22-27 Agosto 2004 Toulouse, France. Edited by J.-J. Levy, E. W. Mayr, J. C. Mitchell. Kluwer, U.S.A. 2004, ISBN:1-4020-8140-5 pp. 23 - 36 (con I. Toli)

⋆ *Numerical Gröbner bases and syzygies: an interval approach.* Proceedings of the 6^{th} SYNASC Symposium. D. Petcu, D. Zaharie, V. Negru, T. Jebelean ed. Timişoara, Romania 2004, pp. 77 - 89, ISBN 973-661-441-7 (con M. Bodrato)

⋆ *Gröbner bases computation using syzygyes: a numerical approach with intervals.* Analele Universităţii de Vest din Timişoara - Seria Matematică–Informatică Vol. XLII, Fasc. special 2, 2004, pp. 13 - 30 (con M. Bodrato)

⋆ *Hilbert Stratification and Parametric Gröbner Bases.* Proceedings of the 8^{th} CASC workshop. V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov ed. Springer-Verlag LNCS 3718. Kalamata, Grecia 2005, ISSN 0302-9743, ISBN 3-540-28966-6, pp. 220-235 (con L. Gonzalez-Vega, C. Traverso)

⋆ *Intervals, Syzygies, Numerical Gröbner Bases : A Mixed Study* Proceedings of the 9^{th} CASC workshop. V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov ed. Springer-Verlag LNCS 4194. Chişinău, Moldova 2006, ISSN 0302-9743, ISBN 3-540-45182-X, pp. 64-76 (con M. Bodrato)

⋆ *What about Toom-Cook matrices optimality ?* Preprint n. 605. Centro Interdipartimentale Vito Volterra, Università di Roma "Tor Vergata", 2006 (con M. Bodrato).

⋆ *Integer and Polynomial Multiplication: Towards Optimal Toom-Cook Matrices* Atti ISSAC 2007, C. W. Brown ed. Waterloo, Ontario, Canada, 2007, ACM press, New York, USA, ISBN 978-1-59593-743-8, pp. 17 - 24 (con M. Bodrato).

⋆ *Some Toom-Cook methods for even long integers* Acta Universitatis Apulensis, Mathematics-Informatics, Special Issue, Proceedings of the International Conference on Theory and Applications of Mathematics and Informatics, ICTAMI 2009. Daniel Breaz, Nicoleta Breaz, Dorin Wainberg editors. Aeternitas Publishing House, Alba Iulia, Romania, settembre 2009, ISSN 1582 - 5329, pp. 807 - 828

⋆ *Iterative Karatsuba method for multivariate polynomial multiplication* Acta Universitatis Apulensis, Mathematics-Informatics, Special Issue, Proceedings of the International Conference on Theory and Applications of Mathematics and Informatics, ICTAMI 2009. Daniel Breaz, Nicoleta Breaz, Dorin Wainberg editors. Aeternitas Publishing House, Alba Iulia, Romania, settembre 2009, ISSN 1582 - 5329, pp. 829 - 843

⋆ *Toom-Cook 8-way for long integers multiplication* Atti 11° Simposio SYNASC. S. Watt, V. Negru, T. Ida, T. Jebelean, D. Petcu, D. Zaharie ed. IEEE, Los Alamitos, USA, settembre 2009, pp. 54-57, ISBN 978-0-7695-3964-5

⋆ *Conjugation as Public Key Agreement Protocol in Mobile Cryptography* Atti dell'International Conference on Security and Cryptography SECRYPT 2010, Atene, Grecia, ISBN 978-989-8425-18-8, pp. 411-416 (con V. Ottaviani, M. Regoli)

⋆ *Iterative Toom-Cook Methods For Very Unbalanced Long Integer Multiplication* Atti ISSAC 2010, Monaco, Germania, 25-28 luglio 2010, ISBN 978-1-4503-0150-3, ACM press, New York, USA, pp. 319-324

⋆ *Karatsuba and Toom-Cook methods for Multivariate Polynomials* Acta Universitatis Apulensis, Mathematics-Informatics, Special Issue, Proceedings of the International Conference on Theory and Applications of Mathematics and Informatics, ICTAMI 2011. Daniel Breaz, Nicoleta Breaz, Nicoleta Ularu, editors. Aeternitas Publishing House, Alba Iulia, Romania, luglio 2011, ISSN 1582-5329, pp. 11-60 (con M. Bodrato)

⋆ *Long Integers and Polynomial Evaluation with Estrin's Scheme* in Proceedings of the 13^{th} SYNASC Symposium, Timişoara, Romania, 26-29 settembre 2011, ISBN 978-0-7695-4630-8 (con M. Bodrato)

⋆ *A new algorithm for long integer cube computation with some insight into higher powers* in Proceedings of CASC 2012, edito da V.P. Gerdt ed al., LNCS 7442, Springer-Verlag, settembre 2012, ISSN 0302-9743, ISBN 978-3-642-32972, pp. 34–46 (con M. Bodrato)

VARIE

Esperienza pluriennale con i linguaggi C, C++ e sviluppo progetti. Conoscenza Java.
Abilitazione per l'insegnamento di Matematica Applicata (A048).
Esaminatore ECDL.
Titolare brevetto RM2011A000641 "Organo di traino per valigie, trolley, carrelli per la spesa e contenitori simili su ruote".

Roma, 1 ottobre 2015