Universiteit
Leiden
The Netherlands

On products of linear error correcting codes

Mirandola, D.

Citation
Mirandola, D. (2017, December 6). *On products of linear error correcting codes*. Retrieved from https://hdl.handle.net/1887/57796

Version:	Not Applicable (or Unknown)
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/57796

Note: To cite this publication please use the final published version (if applicable).

Cover Page

Universiteit Leiden

The handle http://hdl.handle.net/1887/57796 holds various files of this Leiden University dissertation

Author: Mirandola, Diego
Title: On products of linear error correcting codes
Date: 2017-12-06

Bibliography

[1] Mark A. Abspoel. Shamir's scheme is the only strongly multiplicative LSSS with maximal adversary. Master's thesis, Universiteit Leiden, 2016. Preprint: `https://www.math.leidenuniv.nl/scripties/MasterAbspoel.pdf`.

[2] Christine Bachoc, Oriol Serra, and Gilles Zémor. An analogue of Vosper's Theorem for Extension Fields. *Math. Proc. Cambridge Philos. Soc.*, to appear. Preprint: `https://arxiv.org/pdf/1501.00602v1.pdf`, 2015.

[3] Stéphane Ballet and Julia Pieltant. On the Tensor Rank of Multiplication in Any Extension of $\mathbb{F}_2$. *J. Complex.*, 27(2):230–245, April 2011.

[4] Vincent Beck and Cédric Lecouvey. Additive combinatorics methods in associative algebras. Preprint: `https://arxiv.org/pdf/1504.02287v2.pdf`, 2015.

[5] Amos Beimel. *Secure Schemes for Secret Sharing and Key Distribution.* PhD thesis, Technion Haifa, 1996.

[6] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 1–10, New York, NY, USA, 1988. ACM.

[7] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness Theorems for Non-cryptographic Fault-tolerant Distributed Computation. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 1–10, New York, NY, USA, 1988. ACM.

[8] E. Berlekamp, R. J. McEliece, and H. van Tilborg. On the inherent intractability of certain coding problems (Corresp.). *IEEE Transactions on Information Theory*, 24(3):384–386, May 1978.

[9] Koichi Betsumiya, Stelios Georgiou, T. Aaron Gulliver, Masaaki Harada, and Christos Koukouvinos. On self-dual codes over some prime fields. *Discrete Mathematics*, 262(1):37 – 58, 2003.

[10] Andries E. Brouwer, Arjeh M. Cohen, and Arnold Neumaier. *Distance-regular graphs*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer, 1989.

[11] Ignacio Cascudo, Hao Chen, Ronald Cramer, and Chaoping Xing. Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over Any Fixed Finite Field. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009: 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, pages 466–486. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[12] Ignacio Cascudo, Ronald Cramer, Diego Mirandola, Carles Padró, and Chaoping Xing. On secret sharing with nonlinear product reconstruction. *SIAM Journal on Discrete Mathematics*, 29(2):1114–1131, 2015.

[13] Ignacio Cascudo, Ronald Cramer, Diego Mirandola, and Gilles Zémor. Squares of Random Linear Codes. *IEEE Transactions on Information Theory*, 61(3):1159–1173, March 2015.

[14] Ignacio Cascudo, Ronald Cramer, Chaopin Xing, and An Yang. Asymptotic Bound for Multiplication Complexity in the Extensions of Small Finite Fields. *IEEE Transactions on Information Theory*, 58(7):4930–4935, July 2012.

[15] Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, pages 685–705. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[16] Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. The arithmetic codex. In *Information Theory Workshop (ITW), 2012 IEEE*, pages 75–79, Sept. 2012.

[17] Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. Torsion Limits and Riemann-Roch Systems for Function Fields and Applications. *IEEE Transactions on Information Theory*, 60(7):3871–3888, July 2014.

[18] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty Unconditionally Secure Protocols. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 11–19, New York, NY, USA, 1988. ACM.

[19] Hao Chen and Ronald Cramer. Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computations over Small Fields. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006: 26th*

Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006. Proceedings, pages 521–536. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

[20] Hao Chen, Ronald Cramer, Shafi Goldwasser, Robbert de Haan, and Vinod Vaikuntanathan. Secure Computation from Random Error Correcting Codes. In Moni Naor, editor, *Advances in Cryptology - EUROCRYPT 2007: 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007. Proceedings*, pages 291–310. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[21] D. V. Chudnovsky and G. V. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Journal of Complexity*, 4(4):285 – 316, 1988.

[22] Gérard Cohen, Iiro Honkala, Simon Litsyn, and Antoine Lobstein. *Covering Codes*. North-Holland Mathematical Library. Elsevier Science, 1997.

[23] Alain Couvreur, Philippe Gaborit, Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tillich. Distinguisher-based Attacks on Public-key Cryptosystems Using Reed—Solomon Codes. *Des. Codes Cryptography*, 73(2):641–666, November 2014.

[24] Alain Couvreur, Philippe Gaborit, Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tillich. Distinguisher-based attacks on public-key cryptosystems using Reed–Solomon codes. *Designs, Codes and Cryptography*, 73(2):641–666, 2014.

[25] Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich. New Identities Relating Wild Goppa Codes. *Finite Fields Appl.*, 29:178–197, September 2014.

[26] Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich. Polynomial Time Attack on Wild McEliece over Quadratic Extensions. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, pages 17–39. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.

[27] Ronald Cramer, Ivan Damgård, and Ueli Maurer. General Secure Multiparty Computation from any Linear Secret-Sharing Scheme. In Bart Preneel, editor, *Advances in Cryptology — EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000 Proceedings*, pages 316–334. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.

[28] Ronald Cramer, Ivan B. Damgård, and Jesper B. Nielsen. *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, 2015.

[29] Jean Alexandre Dieudonné. *La géométrie des groupes classiques*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, 1971.

[30] Arne Dür. The automorphism groups of Reed-Solomon codes. *Journal of Combinatorial Theory, Series A*, 44(1):69 – 82, 1987.

[31] Iwan M. Duursma and Ralf Kötter. Error-Locating Pairs for Cyclic Codes. *IEEE Transactions on Information Theory*, 40(4):1108–1121, 1994.

[32] Roger H. Dye. On the Arf invariant. *Journal of Algebra*, 53(1):36 – 39, 1978.

[33] Yoshimi Egawa. Association schemes of quadratic forms. *Journal of Combinatorial Theory, Series A*, 38(1):1 – 14, 1985.

[34] Jean-Charles Faugère, Valérie Gauthier-Umaña, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. A Distinguisher for High-Rate McEliece Cryptosystems. *IEEE Transactions on Information Theory*, 59(10):6830–6844, Oct 2013.

[35] Matthew Franklin and Moti Yung. Communication Complexity of Secure Computation (Extended Abstract). In *Proceedings of the Twenty-fourth Annual ACM Symposium on Theory of Computing*, STOC '92, pages 699–710, New York, NY, USA, 1992. ACM.

[36] Xiang-Dong Hou, Ka Hin Leung, and Qing Xiang. A Generalization of an Addition Theorem of Kneser. *Journal of Number Theory*, 97(1):1 – 9, 2002.

[37] W. Cary Huffman and Vera Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2010.

[38] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jürg Wullschleger. Constant-Rate Oblivious Transfer from Noisy Channels. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, pages 667–684. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[39] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge from Secure Multiparty Computation. In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing*, STOC '07, pages 21–30, New York, NY, USA, 2007. ACM.

[40] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-Knowledge Proofs from Secure Multiparty Computation. *SIAM Journal on Computing*, 39(3):1121–1152, 2009.

[41] Johannes H. B. Kemperman. On small sumsets in an abelian group. *Acta Mathematica*, 103(1):63–88, 1960.

[42] Martin Kneser. Abschätzung der asymptotischen Dichte von Summenmengen. *Mathematische Zeitschrift*, 58:459–484, 1953.

[43] Ralf Kötter. A Unified Description of an Error Locating Procedure for Linear Codes. In *Proceedings of the International Workshop on Algebraic and Combinatorial Coding Theory*, pages 113–117, Voneshta Voda, Bulgaria, 1992.

[44] Tsit-Yuen Lam. *Introduction to Quadratic Forms over Fields*. Number 67 in Graduate Studies in Mathematics. American Mathematical Soc., 2005.

[45] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer New York, 2005.

[46] A. Lempel, G. Seroussi, and S. Winograd. On the complexity of multiplication in finite fields. *Theoretical Computer Science*, 22(3):285 – 296, 1983.

[47] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Number 20, pt. 1 in EBL-Schweitzer. Cambridge University Press, 1997.

[48] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The Theory of Error-correcting Codes*. North-Holland mathematical library. North-Holland Publishing Company, 1977.

[49] Irene Márquez-Corbella and Ruud Pellikaan. A Characterization of MDS Codes That Have an Error Correcting Pair. *Finite Fields Appl.*, 40(C):224–245, July 2016.

[50] James L. Massey. Minimal Codewords and Secret Sharing. In *Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory*, pages 269–79, Institutionen för informationsteori, Tekniska högsk. Lund, Sweden, 1993.

[51] James L. Massey. Some Applications of Coding Theory in Cryptography. In *Codes and Ciphers: Cryptography and Coding IV*, pages 33–47, 1995.

[52] R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *DSN Progress Report*, 42–44:114–116, 1978.

[53] Diego Mirandola and Gilles Zémor. Critical Pairs for the Product Singleton Bound. *IEEE Transactions on Information Theory*, 61(9):4928–4937, Sept. 2015.

[54] Melvyn B. Nathanson. *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*. Graduate Texts in Mathematics. Springer New York, 1996.

[55] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information theory*, 15(2):159–166, 1986.

[56] Carles Padró. Lecture Notes in Secret Sharing. `https://mat-web.upc.edu/people/carles.padro/arc02v03.pdf`, 2013.

[57] Ruud Pellikaan. On decoding linear codes by error locating pairs. Preprint: `http://www.win.tue.nl/~ruudp/paper/15-ecp-preprint.pdf`, 1988.

[58] Ruud Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Mathematics*, 106:369 – 381, 1992.

[59] Ruud Pellikaan. On the Efficient Decoding of Algebraic-Geometric Codes. In P. Camion, P. Charpin, and S. Harari, editors, *Eurocode '92: International Symposium on Coding Theory and Applications*, pages 231–253. Springer Vienna, Vienna, 1993.

[60] Ruud Pellikaan. On the existence of error-correcting pairs. *Journal of Statistical Planning and Inference*, 51(2):229–242, 1996.

[61] Hugues Randriambololona. Bilinear Complexity of Algebras and the Chudnovsky-Chudnovsky Interpolation Method. *J. Complex.*, 28(4):489–517, August 2012.

[62] Hugues Randriambololona. An Upper Bound of Singleton Type for Componentwise Products of Linear Codes. *IEEE Transactions on Information Theory*, 59(12):7936–7939, Dec 2013.

[63] Hugues Randriambololona. Asymptotically Good Binary Linear Codes With Asymptotically Good Self-Intersection Spans. *IEEE Transactions on Information Theory*, 59(5):3038–3045, May 2013.

[64] Hugues Randriambololona. Linear independence of rank 1 matrices and the dimension of $*$-products of codes. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 196–200, June 2015.

[65] Hugues Randriambololona. On products and powers of linear codes under componentwise multiplication. *Contemporary Mathematics, Algorithmic Arithmetic, Geometry, and Coding Theory*, 637:3–77, 2015.

[66] Jean-Pierre Serre. *A Course in Arithmetic*. Graduate texts in mathematics. Springer, 1973.

[67] Adi Shamir. How to Share a Secret. *Commun. ACM*, 22(11):612–613, November 1979.

[68] V. M. Sidelnikov and S. O. Shestakov. On insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Mathematics and Applications*, 2(4):439–444, 1992.

[69] Terence Tao and Van H. Vu. *Additive Combinatorics*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[70] J. H. van Lint and R. M. Wilson. On the minimum distance of cyclic codes. *IEEE Transactions on Information Theory*, 32(1):23–40, 1986.

[71] Jacobus Hendricus van Lint. *Introduction to Coding Theory*. Graduate Texts in Mathematics. Springer Berlin Heidelberg, 2013.

[72] A. G. Vosper. The Critical Pairs of Subsets of a Group of Prime Order. *Journal of the London Mathematical Society*, s1-31(2):200–205, 1956.

[73] Christian Wieschebrink. Two NP-complete Problems in Coding Theory with an Application in Code Based Cryptography. In *2006 IEEE International Symposium on Information Theory (ISIT)*, pages 1733–1737, July 2006.

[74] S. Winograd. Some bilinear forms whose multiplicative complexity depends on the field of constants. *Mathematical systems theory*, 10(1):169–180, 1976.