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

Samenvatting

Het product CD van twee codes C en D is gedefiniëerd als het lineair opspansel van alle elementen van de vorm xy, waar x een element van C is en y een element van D, en het product componentbewijs wordt berekend. Het kwadraat C^2 van een code C is op natuurlijke wijze gedefinieerd als het product van C met zichzelf. Deze begrippen zijn de laatste veertig jaar in verscheidene vakgebieden verschenen, zoals in de cryptografie, complexiteitstheorie, additieve combinatoriek en cryptanalyse. We bewijzen drie hoofdresultaten over deze producten en bespreken toepassingen op het gebied van de cryptografie. Onze methoden zijn hoofdzakelijk algebraïsch-combinatorisch, hoewel soms gebruik wordt gemaakt van probabilistische technieken.

Ons eerste doel is om de volgende vraag te beantwoorden: vult het kwadraat van een code "normaliter" de hele ruimte op? We geven een bevestigend antwoord voor codes van dimensie k en lengte ruwweg $k^2/2$ of kleiner. Bovendien is de snelheid van convergentie exponentieel als het verschil $k(k+1)/2 - n$ op zijn minst lineair is in k. Het bewijs gebruikt random codes en combinatorische argumenten, samen met algebraïsche tools die een precieze berekening van het aantal kwadratische vormen van een gegeven rang, samen met hun aantal nulpunten, erbij betrekken. Als gevolg van dit resultaat is het niet mogelijk om random codes te gebruiken in situaties waar bepaalde eisen zijn aan het kwadraat van de code, gezien dat dit met hoge waarschijnlijkheid de hele ruimte zal zijn. Dit heeft gevolgen voor bijvoorbeeld secret sharing: het is bekend dat lineaire, niet-multiplicatieve secret-sharingschema's met optimale privacy- en reconstructieparameters geconstrueerd kunnen worden met random codes; gezien onze resultaten echter, zullen deze schema's hoogstwaarschijnlijk niet aritmetisch zijn.

Ons tweede resultaat karakteriseert product-MDS-paren van lineaire codes, dat wil zeggen paren van codes C, D wier product onder coördinaatsgewijze vermenigvuldiging een maximale minimumafstand heeft als functie van de lengte van de code en de dimensies $\dim C, \dim D$. We bewijzen in het bijzonder voor het geval $C = D$, dat als het kwadraat van de code C een minimumafstand

van op zijn minst 2 heeft, en (C, C) een product-MDS-paar is, dat C ofwel een gegeneraliseerde Reed-Solomoncode is, ofwel C een directe som is van zelfduale codes. Het bewijs is gebaseerd op nieuwe coderingstheoretische analoga van klassieke stellingen uit de additieve combinatoriek, te weten de stellingen van Kneser en Vosper. Recentelijk zijn deze technieken gebruikt om aan de tonen dat, onder alle t-sterk multiplicatieve secret-sharingschema's met n spelers, alleen Shamirs schema de optimale $t = (n-1)/3$ kan bereiken.

Tenslotte richten we ons op een fundamentele vraag die naar ons beste weten nieuw is. Multiplicatieve lineaire secret sharing is een fundamenteel begrip op het gebied van secure multiparty computation, en sinds kort ook op het gebied van twee-spelercryptografie. Kort gezegd geeft dit begrip een garantie dat "het product van twee geheimen verkregen kan worden als een lineaire functie van de vector die bestaat uit het coördinaatsgewijze product van twee respectievelijke share-vectoren". Neem nu aan dat we de conditie van lineariteit laten varen en in plaats daarvan vereisen dat dit product verkregen kan worden door een bepaalde, niet noodzakelijkerwijs lineaire, "productreconstructiefunctie". Is de resulterende notie equivalent met multiplicatieve lineaire secret sharing? We laten het (wellicht contra-intuïtieve) resultaat zien dat deze versoepelde notie een strikte veralgemenisering is. Concreet gezien, neem een eindig lichaam als basislichaam waarover lineaire secret sharing wordt beschouwd. We laten dan zien dat er een (exotisch) lineair secret-sharingschema over dit basislichaam bestaat met een onbegrensd aantal spelers n zodat het t-privacy heeft met $t = \Omega(n)$, en zodat het een productreconstructiefunctie toelaat, waar deze functie noodzakelijkerwijs niet-lineair is. Daarbovenop bepalen we het minimum aantal spelers waarvoor deze exotische schema's bestaan. Ons bewijs is gebaseerd op combinatorische argumenten die betrekking hebben op kwadratische vormen. Het heeft uitbreidingen naar onderscheidingsresultaten voor vergelijkbare versoepelde condities, zoals in het geval van sterk multiplicatieve secret sharing.