On products of linear error correcting codes

Mirandola, D.

Résumé

Le produit CD de deux codes C et D est défini comme l'espace vectoriel engendré par tous les éléments de la forme xy, où x appartient à C, y appartient à D et le produit est effectué coordonnée par coordonnée. Le carré C^2 d'un code C est naturellement défini comme le produit de C par lui-même. Au cours des quarante dernières années, ces notions ont régulièrement fait des apparitions dans différents domaines, comme la cryptographie, la théorie de la complexité, la combinatoire additive et la cryptanalyse. Nous démontrons trois principaux résultats sur les produits de codes et discutons de leurs applications à la cryptographie. Nos méthodes combinent des considérations algébriques et combinatoires, mais parfois des techniques probabilistiques seront également impliquées.

Pour notre premier résultat, notre but principal est de répondre à la question suivante : le carré d'un code "typique", remplit-il l'espace tout entier ? Nous donnons une réponse affirmative, pour des codes de dimension k et de longueur qui ne dépasse pas à peu près $k^2/2$. De plus, la vitesse de convergence vers 1 de la probabilité de cet événement est exponentielle si la différence $k(k+1)/2-n$ est au moins linéaire en k. La preuve utilise du codage aléatoire et des arguments combinatoires, avec des outils algébriques qui impliquent le calcul précis du nombre de formes quadratiques de rang donné, et le nombre de leurs zéros. Comme conséquence de ce travail, il résulte qu'il est impossible de compter sur les codes aléatoires dans des situations où il est nécessaire d'exploiter des propriétés du carré d'un code, car celui-ci sera l'espace entier - donc trivial - avec grande probabilité. Ceci a un impact, par exemple, sur le partage de secret : il est connu que les schémas de partage de secret linéaires non multiplicatifs avec privacy et paramètres de reconstruction optimaux peuvent être construits en utilisant des codes aléatoires ; cependant, nos résultats démontrent que ces schémas seront très probablement non arithmétiques.

Notre deuxième résultat caractérise les paires de codes linéaires Produit-MDS, c'est-à-dire les paires de codes C, D dont le produit coordonnée par coordonnée a la distance minimale la plus grande possible, la longueur des codes et les

dimensions $\dim C, \dim D$ étant fixées. En particulier, nous prouvons que pour $C = D$, si le carré du code C a une distance minimale au moins 2 et (C, C) est une paire Produit-MDS, alors soit C est un code de Reed-Solomon généralisé, soit C est une somme directe de codes autoduaux. La preuve est basée sur des nouveaux résultats de théorie des codes, analogues aux théorèmes classiques de combinatoire additive, notamment ceux de Kneser et de Vosper. Plus récemment, ces techniques ont été utilisées pour montrer que, parmi tous les schémas t-fortement multiplicatifs de partage de secret entre n joueurs, seul le schéma de Shamir peut atteindre le $t = (n-1)/3$ optimal.

Enfin, nous nous concentrons sur une question qui à notre connaissance est nouvelle. Le partage de secret linéaire multiplicatif est une notion fondamentale dans le domaine du calcul sécurisé à plusieurs participants et, depuis peu, dans le domaine de la cryptographie à deux participants aussi. En bref, cette notion guarantit que "le produit de deux secrets est obtenu comme une fonction linéaire du vecteur qui consiste en le produit coordonnée par coordonnée des deux vecteurs de partage respectifs. Supposons que nous renoncions à la condition de linéarité afin de demander plutôt que ce produit soit obtenu par une "fonction de reconstruction du produit" pas forcément linéaire. La notion résultante, est-elle équivalente au partage de secret linéaire ? Nous démontrons le résultat (peut-être quelque peu contre-intuitif) que cette notion relaxée est strictement plus générale. Concrétement, fixons un corps fini comme corps de base sur lequel le partage de secret est défini. Alors nous montrons qu'il existe un schéma de partage de secret linéaire (exotique) avec un nombre illimité de joueurs n, muni de t-privacy avec $t = \Omega(n)$ et qui admet une fonction de reconstruction du produit: mais cette fonction est nécessairement non linéaire. En outre, nous déterminons le nombre minimum de joueurs pour lesquels ces schémas exotiques existent. Notre preuve est basée sur des arguments combinatoires qui impliquent les formes quadratiques. Elle s'étend à des résultats de séparation pour des variations importantes, tels que le partage de secret fortement multiplicatif.