Aix–Marseille Université / Centrale Marseille / CNRS
I2M (Institut de Mathématiques de Marseille), UMR 7373

Mémoire d'Habilitation à Diriger des Recherches

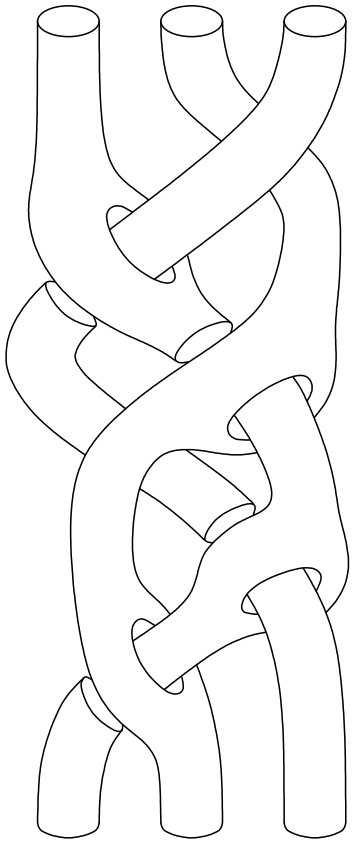
Applications de modèles combinatoires issus de la topologie :

Classification des enlacements d'anneaux à homotopie d'enlacement près
&
Produits et puissances itérées de codes quantiques CSS

présenté publiquement par

Benjamin Audoux

le 16 février 2018



devant le jury

Michel Boileau (tuteur)	Aix–Marseille Université
Seiichi Kamada	Osaka City University
David Kohel	Aix–Marseille Université
Christine Lescop (présidente)	Université Grenoble–Alpes
Peter Teichner	Max Planck Institute
Jean-Pierre Tillich	INRIA de Paris

au vu des rapports de

Seiichi Kamada	Osaka City University
Peter Teichner	Max Planck Institute
Gilles Zémor	Université de Bordeaux

Contents

Remerciements

De tout un mémoire, les remerciements sont, sans conteste, la partie la plus délicate à rédiger. Espérer l'exhaustivité serait utopique et voué sans aucun doute à l'échec. Jouer l'ellipse serait injuste, pour ne pas dire insultant. Car si je suis le seul signataire du présent manuscrit, il n'en est pas moins le fruit de toutes les interactions que j'ai pu avoir, et ce à bien des niveaux.

Il n'y a, à l'évidence, aucun ordre pertinent dans les remerciements. A défaut de pertinence, cherchons donc l'efficience et procédons, autour de l'habilitation, par cercles successifs. Je suis profondément reconnaissant à Christine, David et Jean-Pierre d'avoir accepté de participer à mon jury, me permettant ainsi de montrer l'immense respect que j'ai pour eux et leur travail. Je le suis d'autant plus à Gilles, Seiichi, Peter et Christian qui, en acceptant leur mission de rapporteur ou d'expert, ont pris le temps de se pencher sur mes modestes contributions. Mais bien avant cela, je remercie infiniment Michel de m'avoir soutenu (et poussé) dans cette aventure. Et je remercie également Luisa pour m'avoir entraîné dans cette autre aventure qu'est le mois thématique, lequel a clairement tout accéléré.

Mais bien entendu, il n'y aurait jamais eu non plus d'habilitation s'il n'y a avait pas eu de résultats. Or le vécu des résultats étant tellement plus intense à plusieurs, c'est avec émotions—et ces émotions couvrent tout le spectre de l'affect humain—que je resonge et remercie toutes les personnes avec qui j'ai collaboré. Bien évidemment, je pense à JB, Manu et Paolo qui, avec moi, ont largué les amarres de la caravelle VasKho pour naviguer vers les océans de la dimension quatre[1]; ainsi qu'à Alain qui, lui aussi, a su me pousser vers des eaux nouvelles, aussi bien classiques que quantiques. Et, même si le présent mémoire les passent injustement sous silence, il y a tous mes autres co-auteurs : Ana, Delphine, Enéa, Fionntan, Thomas, Vladimir ; il me faut tout autant les remercier car ce sont toutes ces interactions et toutes ces influences qui ont fait de ce mémoire ce qu'il est, et qui font de ma recherche ce qu'elle sera. Je tiens, au demeurant, à préciser qu'avec toutes ces personnes, mes relations ne se cantonnent pas au strict domaine professionnel, et que ces collaborations seraient certainement restées stériles si elles n'étaient pas pénétrées d'une profonde amitié. Je laisse à chacun le soin d'insérer, ici, son souvenir le plus touchant/amusant/sincère car parmi tous ces bons souvenirs, il me serait trop cruel de choisir.

Mais ces collaborations n'ont pas le pouvoir des iris, elles ne fleurissent pas en terrain aride, et nécessitent pour s'épanouir un terreau fertile et généreux. C'est donc toute une communauté scientifique qu'il me faut encore remercier, car Agnès, Anne-Laure, Anthony, Hoël, Loulou, Nicolas, Pierre, Sebastian, Vladimir et tous les autres, sont autant de personnes dont le contact régulier m'inspire et m'éveille. Et peut-il y avoir épanouissement professionnel sans un environnement bouillonant et chaleureux au quotidien ? L'I2M, qui ne s'appelait pas I2M à l'époque, m'a accueilli en 2010, et les contacts quotidiens avec, parmi beaucoup d'autres, Clothilde, Daniel, David, Erwan, Erwan, Fabien, Jean-Paul, Jean-Yves, Julia, Julien, Nicolas, Nicolas, Pierre sont autant de sources d'amitié et d'échange. Mais dans un laboratoire, il n'y a pas que des chercheurs, fort heureusement, et ma vie ne serait pas si épanouie sans Evelyne, Marie-Christine, Hélène, Valérie, Valérie et, tout particulièrement, Nelly qui m'a supporté durant trois ans de gestion du séminaire GDT.

Brisons un instant et simultanément la dynamique d'expansion circulaire et la règle de non-répétition, pour porter au pinacle Evelyne, Manu et Nina en vertu de toute l'aide qu'ils m'ont apportés dans la dernière ligne droite de la soutenance.

Revenons enfin sur un ultime élargissement du périmètre de gratitude, celui qui retourne aux origines

[1] tant au sens propre qu'au sens imagé de la paternité

et referme la sphère de ma reconnaissance. Je remercie tous mes proches ; mes parents qui, en dépit de mes carences, restent toujours prêts à traverser le département, la région, le pays, pour venir m'épauler ; Cécile, qui pousse la fidélité jusqu'à partager l'intensité d'une nouvelle étape professionnelle, et dont le soutien et les conseils me renforcent au quotidien ; et enfin Eléonore et Sibylle qui, complainte lyrique ou révolutionnaire, me redonnent chaque jour et chaque nuit l'espoir d'un lendemain qui chante.

Avant-propos

Une infusion de menthe poivrée en main[2] et les yeux plongés dans l'âtre, les longues soirées d'hiver sont l'occasion de méditer l'effervescence et l'exaltation des ivresses estivales. Bilan d'une année passée, elles forment la matrice des ambitions naissantes et bâtissent le socle des triomphes à venir. Si seulement la recherche fonctionnait ainsi. Mais la recherche est souvent une course passionée où le chercheur, slalomant entre ses enseignements, ses responsabilités et sa famille, poursuit les veines du filon de ses pensées, bifurquant au gré des rencontres, des envies, des projets. Le tout forme un ensemble cohérent, mais c'est seulement en prenant le temps d'observer ses réalisations que le chercheur peut en respirer l'harmonie. L'habilitation à diriger des recherches est le moment d'une telle suspension.

Ainsi, la réalisation de ce mémoire a été l'occasion d'analyser les forces souterraines qui ont animé mes recherches depuis leurs débuts. La théorie des nœuds reste, sans conteste, un pilier central. Mais au gré de quelques méandres fondateurs, un schéma plus précis s'est dessiné : l'analyse des modèles combinatoires issus de la topologie et leur réutilisation hors de leur contexte originel. Les deux parties qui forment ce mémoire en sont deux illustrations concrètes.

[2] que l'on pourra avantageusement remplacer par un verre de cognac Grand Breuil XO

Introductions

Introduction en français

La théorie des nœuds et des entrelacs étudie, à déformation près, les plongements lisses d'un ou de plusieurs cercles dans S^3. Dès son origine, elle puise ses motivations dans ses applications aux autres domaines. C'est en effet Lord Kelvin qui, le premier, chercha à classifier les nœuds dans la cadre de sa théorie, physique, des atomes-vortex. Tait donna alors les premières tables de classification [Tai84], mais pour une analyse plus intrinsèque, il faut attendre la toute fin du XIX$^{\text{ème}}$ siècle, où l'émergence d'outils algébriques, aussi bien homotopiques qu'homologiques, donnèrent à l'étude des nœuds une nouvelle impulsion. La notion d'extérieur d'un entrelacs, notamment, pris une importance décisive, que ce soit pour l'étude même de l'entrelacs—via, par exemple, l'étude de son groupe fondamental, de ses surfaces proprement plongées et de leurs caractéristiques, ou de ses revêtements qui mènent, entre autre, au polynôme d'Alexander [Ale28]—ou pour ses applications à l'étude des 3–variétés via les techniques de chirurgie. Dès ces débuts, une dimension combinatoire s'est imposée : en projetant génériquement les entrelacs dans un plan et en munissant les points doubles d'une information dessus/dessous, K. Reidemeister réduit en effet l'étude des entrelacs à celle de leurs *diagrammes* modulo trois mouvements locaux [Rei27].

Cette perspective combinatoire s'est ensuite accentuée, au gré des révolutions successives que la théorie des nœuds a traversé. La découverte du polynôme de Jones [Jon87] marque, au milieu des années 80, l'avènement des invariants dits *quantiques*. En prenant une certaine distance vis-à-vis de la topologie, ces derniers renforcent la composante combinatoire de l'étude des entrelacs en s'appuyant sur les diagrammes pour introduire de nouveaux outils, issus des représentations des groupes quantiques. L'idée n'est alors plus nécessairement de définir globalement un invariant, mais de le caractériser localement par une relation dite *d'écheveau* (skein) imposant son comportement vis-à-vis de certains mouvements sur les diagrammes. Notons alors une nouvelle confluence de la théorie des nœuds avec la physique, la construction des invariants de N. Reshetikhin et V. Turaev, étendus au cas des graphes rubans dans [RT90], s'inspirant en effet fortement d'une interprétation du polynôme de Jones, donnée par E. Witten [Wit94], dans le cadre physique de la théorie quantique des champs.

La théorie des *invariants de type fini*, également appelés *invariants de Vassiliev*, a accentué, au début des années 90, ce virage combinatoire en intégrant les invariants quantiques au sein d'une famille plus vaste. Cette dernière est définie en considèrant l'espace des nœuds longs immergés et en regardant les cocycles modulo les différentes strates induites par le nombre de points singuliers ; V. Vassiliev définit ainsi des invariants de différents degrés [Vas90]. Cette construction a ensuite été réinterprétée par M. Goussarov [Gou94], et indépendamment par J. Birman et X-S. Lin [BL93], comme l'ensemble des invariants ayant un comportement polynomiale, dans le sens où une certaine dérivée itérée s'annule, la dérivation correspondant ici à la différentiation de l'invariant entre deux entrelacs obtenus l'un par rapport à l'autre par un unique changement de croisement. Les invariants de type fini induisent une filtration sur le module abstraitement engendré par les entrelacs, et l'étude de ces invariants peut se ramener à l'étude de l'espace gradué $\mathcal{G}$ associé, et plus précisemment à la recherche d'une base combinatoire pour $\mathcal{G}$; voir [Bar95]. En quelques années, le nombre d'invariants connus et étudiés a donc explosé, mais la plupart d'entre eux restent topologiquement mystérieux, les liens avec les invariants classiques demeurant largement incompris.

A l'aube du XX$^{\text{ème}}$ siècle, une nouvelle direction s'est ouverte pour l'étude des invariants quantiques, non plus en élargissant leur famille, mais en les raffinant, au contraire, chacun indépendamment. Là encore, tout commença par le polynôme de Jones et sa *catégorification*, l'homologie de Khovanov : de manière

combinatoire, M. Khovanov [Kho00] définit un invariant prenant la forme d'une homologie bigraduée dont la caractéristique d'Euler graduée redonne le polynôme de Jones. Le polynôme d'Alexander fut ensuite, lui aussi, rapidement catégorifié par P. Ozsváth, Z. Szabó [OS04] et, indépendamment, J. Rasmussen [Ras03], sous le nom d'homologie d'Heegaard–Floer. D'autres invariants quantiques suivirent. Outre leur capacité accrue à distinguer les nœuds entre eux, les différentes catégorifications se distinguent, en général, par leur comportement fonctoriel vis-à-vis des cobordismes de nœuds, offrant ainsi aux invariants quantiques une interprétation d'ordre catégorique. Dans ce contexte également, le travail consiste pour beaucoup à identifier des objets de type algébrique reproduisant combinatoirement la relation d'écheveau de l'invariant catégorifié. Notons toutefois le caractère singulier de l'homologie d'Heegaard–Floer, de part sa contruction—relevant de la géométrie symplectique et des A_∞–structures—et de part sa surprenante capacité à détecter les propriétés topologiques d'un nœud.

Mes travaux de thèse, puis de postdoc, se sont inscrits dans ce contexte de catégorification. Un premier pan visait à décortiquer les mécanismes internes d'invariance de l'homologie de Khovanov ; cela a mené à un raffinement trigradué de cette dernière pour des notions d'entrelacs contraints [14, 13, 11]. Un second pan, plus ambitieux, cherchait à identifer certains comportements de type fini au sein de l'homologie de Heegaard–Floer ; cela a mené, en particulier, à une extension de cette dernière aux entrelacs singuliers[3] [12]. Ces années m'ont permis d'assimiler différentes structures combinatoires, toutes issus de la topologie.

Suite à mon recrutement à l'Université d'Aix–Marseille en 2010, le spectre de ma recherche s'est élargi, et son optique s'est, en un sens, inversé : une large proportion de mes travaux s'attache désormais à réutiliser des modèles combinatoires ou des outils issus de la théorie des nœuds dans d'autres domaines, connexes ou plus lointains. Dans ce mémoire, j'ai décidé de développer deux aspects distincts. Le premier concerne la classification des anneaux proprement plongés dans B^4 à homotopie d'enlacement près. Un élément clef de cette classification provient de l'identification d'une sous-classe—celle des anneaux rubans—dont le comportement reproduit celui des enlacements d'intervalles classiques. Le second porte sur les codes correcteurs d'erreurs quantiques dits CSS, leur réinterprétation en terme de complexes de chaînes sur $\mathbb{F}_2$, et comment ce pont permet de définir et d'étudier une notion de produit pour les codes CSS.

Application des enlacements d'intervalles aux anneaux proprement plongés dans B^4

Comme rappelé au début de cette introduction, la théorie des nœuds consiste à étudier les différentes façons qu'un cercle plongé dans S^3 a de se nouer avec lui-même. L'étude des entrelacs procède de même avec plusieurs cercles. Mais dans ce second cas, plusieurs phénomènes se mêlent, les différentes composantes pouvant s'enlacer entre elles, mais chaque composante pouvant également se nouer toute seule. En autorisant chaque composante connexe à s'auto-croiser, la notion d'*homotopie d'enlacement* (link-homotopy), introduite par J. Milnor dans sa thèse, permet de se concentrer uniquement sur l'enlacement des composantes distinctes entre elles. Dans l'objectif d'une classification complète, J. Milnor a montré [Mil54] le rôle essentiel joué par l'image des *longitudes* dans le quotient du groupe fondamental par les différents termes de sa suite centrale descendante. De ces éléments, il extrait une suite de nombres, dits *de Milnor*, dont certains, dits *sans répétition*, sont invariants par homotopie d'enlacement. Ces nombres ne sont toutefois définis que modulo une certaine quantité, déterminée par les nombres de Milnor d'ordre inférieur.

Quelques trente ans plus tard, N. Habegger et X-S. Lin ont étendu les travaux de J. Milnor au cas des *enlacements d'intervalles* (string links). Ces derniers correspondent aux plongements de segments compacts dans B^3 à bords fixés dans ∂B^3. En recollant de manière standard les extrémités de chacun de ses composantes, tout enlacement d'intervalle se referme en un entrelacs ; et inversement, tout entrelacs peut s'ouvrir en un enlacement d'intervalles. Cette correspondance n'est cependant pas bijective et les clôtures d'enlacements d'intervalles distincts peuvent donner le même entrelacs. Dans le cas des enlacements d'intervalles, les nombres de Milnor sont cependant parfaitement définis, l'indétermination dans le cas des entrelacs correspondant à l'indétermination de leur ouverture en enlacement d'intervalles. Dans [HL90], N. Habegger et X-S. Lin montrent que les enlacement d'intervalles sont, à homotopie d'enlacement près, équivalents aux tresses et que ces dernières sont classifiées, toujours à homotopie d'enlacement près, par les nombres de Milnor sans répétition. Bien qu'équivalent, l'invariant classifiant de Habegger–Lin prend

[3] au sens de Vassiliev

néanmoins une autre forme, celle d'un automorphisme *à base conjugante* (basis-conjugating) du groupe libre réduit RF_n, généralisant ainsi les représentations d'Artin pour les groupes de tresses [Art47].

A l'instar des entrelacs, les enlacements d'intervalles peuvent s'étudier via leurs diagrammes modulo les mouvements de Reidemeister. L'homotopie d'enlacement, elle aussi, peut rentrer dans ce cadre comme la relation d'équivalence induite par le *changement d'auto-croisement* (self–crossing change), à savoir l'opération qui échange l'information dessus/dessous sur un point double dont les deux préimages sont sur la même composante.

D'un point de vue combinatoire, les diagrammes d'entrelacs peuvent s'interpréter comme des graphes planaires 4-valents et les différents mouvements comme des opérations locales sur ces graphes. En relâchant la condition de planarité, on définit les objets *virtuels*. Bien que de nature purement diagrammatique, de nombreux invariants d'ordre topologique s'étendent au cas virtuel. La *présentation de Wirtinger* du groupe fondamental, construite combinatoirement sur la donnée d'un diagramme, s'étend par exemple sans difficulté au cas virtuel. Il est notable qu'une majorité de ces invariants topologiques étendus combinatoirement se révèlent invariants par un certain mouvement local, noté OC (over-commute) dans la suite. La théorie des nœuds *soudés* (welded) est définie comme le quotient de la théorie virtuelle par ce mouvement OC. Comme nous allons le voir, cette définition, *a priori* arbitraire, se justifie topologiquement au niveau des surfaces nouées dans B^4 comme la combinatoire de singularités 4-valentes en dimension plus grande.

La théorie des surfaces nouées en dimension 4 trouve son origine au milieu des années 20, dans les travaux de E. Artin [Art25]. L'étude systématique de ces objets ne commença néanmoins qu'au début des années 60, notamment avec les travaux de M. Kervaire, R. Fox et J. Milnor [FM66, KM61, Ker65], mais aussi de T. Yajima ou T. Yanagawa, au Japon[4]. Dès ces débuts, on peut identifier deux approches pour l'étude des surfaces. Un premier courant, issu des dimensions supérieures, s'inscrit dans une perspective fortement algébrique; un second, issu de la dimension 3, reprend de la théorie des nœuds les aspects diagrammatiques. A l'image des entrelacs, les surfaces nouées peuvent en effet s'étudier au travers de leurs projections génériques, mais le jeu des singularités apparaissant après projection est alors plus complexe : on y retrouve des lieux de points doubles, mais aussi des points triples et des points de branchement. Néanmoins, en se limitant aux diagrammes ne possédant que des lieux de points doubles, la combinatoire obtenue se rapproche fortement de celle des entrelacs ; cela fut remarqué par T. Yajima [Yaj62] *via* l'application Tube, laquelle gonfle combinatoirement tout diagramme d'entrelacs en tores noués ou, de manière équivalente, *via* l'application Spun, qui associe à un entrelacs la réunion de ses images par rotation autour d'un axe. Dans le cas des sphères, T. Yanagawa montra que la sous-classe des surfaces possédant un diagramme sans point triple ni point de branchement, initialement appelée *simple*, s'identifie à une autre sous-classe, celle des surfaces *rubans*, définie de manière plus topologique comme les surfaces bordant une 3–boule immergée dont le lieu singulier se limite à un certain type de singularités dites *rubans* [Yan69a, Yan69b, Yan70]. Dans le cas des tores, la classe ruban est plus restrictive que la classe simple, mais c'est précisément dans celle-ci que les applications Tube et Spun plongent la théorie des entrelacs classiques. En 2000, S. Satoh a montré [Sat00] que l'application Tube pouvait même s'étendre—au prix de son injectivité—en une application surjective définie des entrelacs soudés vers les tores rubans.

L'application Tube fait donc le lien entre la théorie soudée—laquelle peut-être vue comme une extension combinatoire de la théorie des nœuds—et la théorie ruban—laquelle peut-être vue comme une étape intermédiaire vers la théorie générale des surfaces nouées. C'est en s'appuyant sur ce parallèle que les travaux présentés dans la première partie généralisent la théorie de Habegger–Lin à la dimension 4. Nous y introduisons les *enlacements d'anneaux* (string 2–link), définis comme les anneaux proprement plongés dans B^4 à bords trivialement fixées dans $\partial B^4 \cong S^3$, et les classifions à homotopie d'enlacement près. La preuve s'articule en trois étapes. Dans un premier temps, le résultat est montré au sein de la sous-classe ruban, pour une notion *a priori* restreinte d'homotopie d'enlacement ruban. Puis dans un second temps, nous montrons un résultat de généricité pour la sous-classe ruban, dans le sens où tout enlacement d'anneaux est, à homotopie d'enlacement près, équivalent à un enlacement d'anneaux ruban. Enfin, nous montrons que l'invariant classifiant pour la sous-classe ruban est invariant par homotopie d'enlacement générale.

[4] voir plus bas pour des références, et [Suz76] pour une bilbiographie plus exhaustive

Pour la première étape, nous commençons par réduire les enlacements d'intervalles classiques à la simple donnée, pour un diagramme fixé, des interconnexions entre ses points doubles vues comme des singularités 4–valentes. Par un procédé de coloriage de ce substrat combinatoire par des éléments de RF_n, nous en déduisons une construction alternative de l'invariant de Habegger–Lin. Cette construction s'étend dès lors au cas soudé, et donc au cas ruban. Nous profitons d'ailleurs de ce mémoire pour traiter, plus généralement, le cas ruban de codimension deux en toute dimension supérieure.

Les deux étapes suivantes s'appuient fortement sur la notion de diagramme pour les surfaces nouées (broken surface diagram) ; mais cela présente une difficulté nouvelle pour traiter les homotopies d'enlacement. En effet, dans le cas de la dimension 3, tout enlacement d'intervalle singulier peut être localement désingularisé par une perturbation infinitésimale, et la notion d'homotopie d'enlacement se réduit à un mouvement supplémentaire sur les diagrammes réguliers. En dimension 4, une surface singulière générique possède un nombre fini de points doubles isolés robustes à toute perturbation. Nous commençons donc par développer une théorie de diagramme pour les surface immergées, et nous donnons trois mouvements singuliers qui, complétés par les *mouvements de Roseman* du cas plongé, génèrent l'homotopie d'enlacement. Au passage, nous donnons également des jeux de mouvements générant, respectivement, l'isotopie ambiante pour les surfaces singulières, l'homotopie régulière et l'homotopie générale. A l'aide de ces diagrammes de surfaces singulières et encore par un procédé de coloriage par des éléments de RF_n, nous étendons l'invariant de Habegger–Lin à tous les enlacements d'anneaux immergés, et montrons qu'il est invariant par homotopie d'enlacement. Toujours à l'aide des diagrammes de surfaces immergées nous montrons également que le résultat de généricité sur les objets rubans évoqué plus haut est équivalent à un théorème de A. Bartels et P. Teichner affirmant que tout plongement de sphères dans S^4 est trivial à homotopie d'enlacement près [BT99].

Comparé au résultat de Habbeger–Lin et aux travaux de J. Milnor, le théorème de Bartels–Teichner semble indiquer une rupture de comportement entre la dimension 3 et la dimension 4. Il n'en est rien. La classification des entrelacs et des enlacements d'intervalles se cristallise en effet sur la notion de longitude pour ces objets ; or les sphères, étant simplement connexes, n'ont pas de longitude. Il est donc bien plus naturel de voir la classification des entrelacs s'étendre aux tores noués plutôt qu'aux sphères. C'est tout du moins la philosophie qui sous-tend la généralisation de la classification de Habbeger–Lin à la dimension 4 développée dans ce mémoire.

Application de la topologie algébrique aux codes quantiques

En informatique, les codes correcteurs d'erreurs ont été développés afin de détecter et de corriger les éventuelles erreurs pouvant apparaitre lors de la transmission d'un message. La stratégie consiste à plonger l'ensemble des mots possibles, vu comme un $\mathbb{F}_2$–espace vectoriel, dans un espace plus grand afin d'enrober tout message d'une certaine redondance. Tous les codes correcteurs ne se valent pas, et les paramètres les plus élémentaires permettant de les comparer sont leurs *longueurs*, correspondant à la taille des mots après encodage, leurs *dimensions*, correspondant à la taille des mots avant encodage, et leurs *distances minimales*, qui quantifie le nombre d'erreurs corrigibles. Par ailleurs, le décodage d'un code général étant NP–complet [BMv78], l'existence d'algorithmes de décodage efficaces[5] pour un code donné est également un aspect essentiel. De ce point de vue, les codes *LDPC*, introduits par R. Gallager dans sa thèse [Gal62], se sont particulièrement distingués : certains *algorithmes de décodage itératif* [RSU01] peuvent alors s'appliquer avec une complexité très faible, des performances proches de la limite de Shannon, et ce sur des familles dont les dimensions et distances minimales augmentent linéairement avec la longueur.

En informatique quantique, la correction d'erreur est, d'une part, d'autant plus essentielle que le simple stockage de donnée est inévitablement soumis à des phénomènes naturels de décohérence mais, d'autre part, également compromise par le théorème d'impossibilité du clonage quantique. Longtemps considéré comme insurmontable, A. R. Calderbank, P. Shor [CS96] et, indépendamment, A. Steane [Ste96] ont néanmoins réussi à contourner le problème en élaborant un système de codage, dit *stabilisateur*, permettant une procédure quantique de correction d'erreur. Parmi ces codes stabilisateurs, Calderbank–Shor et Steane ont plus particulièrement mis en lumière les codes dits *CSS*. En dépit des différences profondes entre les théories classiques et quantiques des codes correcteurs, on retrouve, pour les codes CSS, les notions de

[5] de complexité polynômiale

longueur, de dimension, de distance minimale, et même le caractère LDPC, qui ne facilite plus seulement l'émergence d'algorithme performant de décodage [PC08], mais aussi, en minimisant le nombre de qubits susceptibles d'interagir, l'implémentation concrète du codage. Plus important encore, la donnée d'un code CSS équivaut à la donnée de deux codes classiques orthogonaux, ce qui fournit un angle d'attaque naturel pour les théoriciens des codes. De ce point de vue, la longueur et la dimension du code CSS se déduisent aisément de celles des deux codes classiques, mais la distance minimale, elle, n'est que minorée. Cela a néanmoins donné lieu à de nombreuses familles LDPC de codes quantiques, on pourra citer par exemple [Pos01], [MMM04], [COT07], [GFL08], [Hag08], [IM07], [Djo08], [SRK08], [Aly08], [AMT12], [TZ14], [CDZ13] ou [Del12].

Mais la donnée d'un code CSS, combinatoirement, correspond également à la donnée d'un complexe de chaînes de longueur trois muni d'une base. Le parallèle va même plus loin : la longueur du code associé à un complexe de chaîne correspond à la dimension de l'espace central du complexe, la dimension à celle de l'homologie et la distance minimale au poids minimal d'un représentant d'une classe non triviale en homologie ou en cohomologie. Cette convergence des codes quantiques et de la topologie (algébrique), inattendue mais observée très tôt par A. Kitaev, est à l'origine de plusieurs constructions de codes. Là aussi, on pourra citer [Kit03], [FM01], [FLM02], [BMD07], [Zém09] ou [10] pour autant de familles, toutes LDPC.

De nombreuses familles LDPC de codes CSS sont donc connues, basées sur des constructions très différentes les unes des autres. Un fait remarquable les unit : contrairement au cas classique, aucune ne possède une distance minimale augmentant plus vite que la puissance $\alpha^{\text{ième}}$ de la longueur, avec $\alpha > \frac{1}{2}$. De ce point de vue, les deux meilleures familles sont celle de Freedman–Luo–Meyer, dont la dimension augmente comme $\sqrt{n}$ et la distance minimale comme $\sqrt{n\sqrt{\ln(n)}}$ où n est la longueur; et celles de Tillich–Zémor, dont la dimension est linéaire en la longueur et la distance minimale augmente comme la racine carrée de la longueur. Le caractère fortuit ou non de cette barrière pour la distance minimale en racine carrée de la longueur reste à ce jour une question ouverte, et beaucoup d'efforts sont actuellement développés pour construire des familles LDPC la dépassant. C'est dans cet objectif, et avec l'idée de considérer des familles de puissances itérées, que les travaux qui suivent ont été initiés.

Les résultats présentés dans la seconde partie de ce mémoire visent à approfondir le parallèle entre codes CSS et complexes de chaînes en cherchant, plus particulièrement, à exporter la notion de produit tensoriel $\otimes$, définie pour les seconds, vers les premiers. Implicite dans de nombreuses constructions, nous lui donnons ici un cadre formel. Il en résulte deux notions de produit pour les codes CSS, une version standard $\otimes$, et une version réduite $\otimes_r$ pour laquelle la longueur est légèrement améliorée. Notons que, dans [BH14], S. Bravyi et M. Hastings introduisent également une notion de produit homologique $\boxtimes$ pour une sous-classe des codes CSS ; bien que distinctes, les produits $\otimes$ et $\boxtimes$ sont fortement liées.

Pour les produits $\otimes$ et $\otimes_r$, ainsi que leurs puissances itérées, nous étudions les paramètres résultants. Nous obtenons des formules exactes pour les longueurs et les dimensions, mais les distances minimales restent difficile à contrôler. Nous fournissons néanmoins, et c'est là le résultat principal de cette seconde partie, un critère de nature cohomologique permettant d'obtenir une borne inférieure sur la distance minimale d'un produit de codes, le produit pouvant être $\otimes$, $\otimes_r$ ou $\boxtimes$. Il était globalement connu, ou tout du moins attendu, que pour deux codes $\mathcal{C}$ et $\mathcal{D}$, la distance minimale du produit était plus grande que chacune des distances minimales $d_{\mathcal{C}}$ et $d_{\mathcal{D}}$. Mieux que cela, nous obtenons comme corollaire de notre critère que, sauf dans certains cas triviaux,

$$d_{\mathcal{C}\otimes\mathcal{D}}, d_{\mathcal{C}\otimes_r\mathcal{D}}, d_{\mathcal{C}\boxtimes\mathcal{D}} \geq 2\max(d_{\mathcal{C}}, d_{\mathcal{D}}).$$

En particulier, les puissances itérées de n'importe quel code honnête donnent une famille LDPC dont la distance minimale tend exponentiellement vers l'infini. Et plus surprenamment encore, un phénomène de *dégénérescence quantique*—c'est-à-dire, pour un code CSS vu comme deux codes classiques $\mathcal{C}_1$ et $\mathcal{C}_2$ orthogonaux, une distance minimale strictement plus grande que chacune des distances minimales de $\mathcal{C}_1$ et $\mathcal{C}_2$—apparait nécessairement pour les puissances assez grande, même s'il est absent du code de départ.

A l'aide de notre critère, nous retrouvons les codes de J-P. Tillich et G. Zémor [TZ14]. Nous retrouvons également certains codes de Khovanov, construits dans [10] ; nous en profitons d'ailleurs pour redonner leur définition dans ce mémoire car c'est aussi un exemple de transport d'un certain modèle combinatoire, celui des complexes de chaînes de Khovanov, vers un autre domaine, celui des codes CSS. Nous discutons

également les liens forts entre $\otimes$ et $\boxtimes$, montrant comment l'un peut se déduire de l'autre. Et enfin, nous donnons trois nouvelles séries de familles LDPC de codes CSS basées, respectivement, sur la géométrie projective finie, les codes cycliques et les codes de Reed–Muller. Ces trois situations ont en commun d'avoir un large groupe d'automorphismes, ce qui favorise l'utilisation de notre critère. Parmi ces familles, la meilleure permet d'extraire une sous-famille quasi-LDPC, dans le sens où le poids augmente plus lentement que n'importe quelle puissance positive de la longueur, dont la dimension augmente plus vite que la puissance $\alpha^{\text{ième}}$ et la distance minimale plus vite que la puissance $\beta^{\text{ième}}$ de la longueur, pour n'importe quels $\alpha < 1$ et $\beta < \frac{1}{2}$; laissant, de fait, la question de la barrière en racine carrée toujours ouverte.

English introduction

Knot and link theory studies, up to deformation, smooth embeddings of one or several copies of S^1 in S^3. From its early days, it was motivated by its applications to other fields. Lord Kelvin initiated indeed the first attempt to classify knots whithin the framing of its vortex theory of atoms. Tait provided then the first knots table [Tai84], but it's only at the very end of the XIX$^{\text{th}}$ century that a more intrinsic study has begun, with new homotopical and homological tools, emerging from algebra. In particular, knot complements became a key notion not only for the direct study of links—through, for instance, the study of their fundamental groups, of their properly embedded surfaces and their characteristics, or of their coverings which led, among other, to the Alexander polynomial [Ale28]—but also for the study of 3–manifolds through surgery technics. At this stage, combinatorial considerations were already on the table: with generic planar projections, enhanced with an over/under data for each double point, K. Reidemeister reduced indeed the link theory to the study of link *diagrams* up to three local moves [Rei27].

Then, most of the main breakthroughs of the last decades brought to light new combinatorial aspects of knot theory. Jones polynomial [Jon87], in the mid 80$^{\text{ies}}$, initiated the development of the, so-called, *quantum invariants*. Walking somehow away from topology, these invariants rely on understanding how the structure of quantum groups can be incarnated by diagram combinatorics. Invariants are then not necessarily defined at once, but characterized by some local *skein* relations which prescribe the invariant behavior with regard to some moves on diagrams. It should be noted, here, a second convergence of knot and physical theories, the construction of N. Reshetikhin and V. Turaev's invariants, extended to ribbon graphs in [RT90], being indeed largely motivated by E. Witten's interpretation of the Jones polynomial within the quantum field theory framework.

In the early 90$^{\text{ies}}$, the theory of *finite type invariants*, also called *Vassiliev invariants*, widened the scope of combinatorics within knot theory by including quantum invariants inside a larger class of invariants. First introduced by V. Vassiliev [Vas90] as cocyles in the space of immersed long knots, modulo the strata induced by the number of singular points, finite type invariants were then reinterpreted by M. Goussarov [Gou94], and independently by J. Birman and X-S. Lin [BL93], as the set of invariants having a polynomial behavior, in the sense that they vanishe after a certain number of iterated derivation; the derivation, here, corresponds to the differentitation of the invariant evaluated on two links which differ one from the other by exactly one crossing change. Finite type invariants induce a filtration on the module abstractly spanned by links, and the study of these invariants boils down to the study of the associated graded space $\mathcal{G}$, and more precisely to the search of a combinatorial basis for $\mathcal{G}$; see [Bar95]. In a few decades, the number of studied invariants has hence substantially increased, but most of them remain topologically mysterious, the connections between them and classical invariants being still misunderstood.

At the turn of the XX$^{\text{th}}$ century, a new dawn appeared for quantum invariants, not anymore by enlarging their family, but on the contrary, by refining them independently. Again, the story began with the Jones polynomial and its *categorification*, Khovanov homology: in a combinatorial way, M. Khovanov [Kho00] defined a new invariant, shaped as bigraded homology groups, whose graded Euler characteristic recovers the Jones polynomial. Soon after, Alexander polynomial was categorified by P. Ozsváth, Z. Szabó [OS04] and, independently, J. Rasmussen [Ras03], under the name of Heegaard–Floer homology. More invariants followed. Besides their increased ability to detect links, categorifications distinguish themselves by their functorial behavior with regard to knot cobordisms, and this provides a categorical interpretation to quantum

invariants. In this categorification setting, a large part of the work is to identify some algebraic objects which combinatorially reproduce the diagrams skein relations. At this point, the singular case of Heegaard–Floer homology should be emphasized, singular because of its construction—based on symplectic geometry and A_∞–structures—but also singular for its remarkable capacity to detect topological properties of knots.

My research, during my PhD and, then, during my postdoc years, fitted within this categorification framework. It began with a carefull analysis of internal mechanisms of invariance in Khovanov homology; this led to a triply graded refinement for some restricted notion of knots [14, 13, 11]. A second, more challenging, stage aimed at determining, within Heegaard–Floer homology, some finite type behaviors; it led to an extension of Heegaard–Floer homology to singular links[6] [12]. During these years, I assimilated several combinatorial structures, all emerging from topology.

Since my position as Maître de conférence at Aix–Marseille University, in 2010, the scope of my research widened and its perspective has somehow reversed: a large part of my work focus now on recycling combinatorial models or tools coming from knot theory to handle questions in other fields, that may be topological or not. In this dissertation, I have decided to develop two distinct aspects. The first one concerns the classification of knotted annuli in B^4 up to link-homotopy; a key point of this classification is the identification of a subclass—the ribbon subclass—whose behavior reproduces classical string links behavior. The second deals with, so-called, CSS quantum error-correcting codes, their interpretation as chain complexes over $\mathbb{F}_2$, and how this bridge can be used to define and study a product notion for CSS codes.

[6] in Vassiliev sense

Overview of the personal works

Along the present dissertation, the author's papers are referenced by numbers whereas other papers are referenced by names in lexicographical order.

During his PhD and the subsequent postdocs, the author's work was essentially focussed on categorification of link invariants. Among his papers:

- [14, 13, 11] concern refinments of Khovanov homology to several restricted notions of links;
- [12] concerns a generalization of Heegaard–Floer homology to singular links, seen from the Vassiliev point of view, motivated by the foundation of a first bridge between categorification and finite type invariants.

After being hired in Aix–Marseille University, the scope of the author's research has been broadened to include other topological topics—such as knotted surfaces or 3–manifolds finite type theories—but also applications of topology in other fields of mathematics—such as quantum correcting codes or eigenvalues of p–Laplacian. Among his papers:

- [8, 9, 7, 5, 6] concern essentially welded knot theory, its relations to classical and virtual knot theories and its applications to knotted surfaces;
- [10, 2] concern CSS quantum codes seen from a topological point of view;
- [3] is an enumeration of hyperbolic knots obtained by surgery on the twisted 5–chain link which realize maximal distances between exceptional slopes;
- [4] uses topological methods to study multiplicity and symmetry of higher eigenvalues and eigenfunctions of the p–Laplacian;
- [1] investigates the injectivity status of some maps between beaded Jacobi diagrams with the aim of establishing the universality of both the Kricker lift of the Kontsevich integral and the Lescop equivariant invariants among finite type invariants, with respect to null-moves, of $\mathbb{Q}$SK–pairs, which are null-homologous knots in rational homology 3–sphere.

Regarding the present dissertation:

- [8] is covered in Sections 2 and 3 of the first part;
- [9] is essentially covered in Section 3 of the first part;
- [6] is covered in Sections 3 and 4 of the first part;
- [2] is covered in the second part;
- [10] is covered in Section 3.2 of the second part;
- even though closely related to the first part, [7, 5] are not developped;
- [14, 13, 11], [12], [3], [4] and [1] are not discussed, even if they are all either developping combinatorics emerging from topology, or applying topology to handle questions in an other field of mathematics.

Chapter I

From topology to topology via combinatorics

Introduction

Knot theory studies how an embedded circle in S^3 can knot itself. Link theory does the same with several circles. But in the latter case, one can distinguish two distinct phenomena: linkedness which is how distinct components are linked, and knottedness which is how each component additionally knots itself. In order to focus on linkedness only, J. Milnor introduced the notion of *link-homotopy* which allows every component to cross itself. In rough words, links up to link-homotopy corresponds to the link theory quotiented by the knot theory. With the aim of giving a complete classification, J. Milnor highlighted in [Mil54] the key role played by the image of *longitudes* in the fundamental group quotiented by the various terms of its central series. From these elements, he deduced a sequence of numbers—the *Milnor numbers*—among which, some—the *non repeating* ones—are invariant under link-homotopy. These numbers are however defined only up to some undeterminacy, which depends on Milnor numbers of lower degree.

Some thirty years later, N. Habegger et X-S. Lin extended J. Milnor's work to the case of *string links*, which are knotted strings in B^3 with fixed extremities on ∂B^3. By gluing together the extremities of each string in a prescribed trivial way, one can close any string link into a link; and reciprocally, any link can be cut open into a string link. But the correspondence between links and string links is not one-to-one, and the closure of distinct string links can be isotopic. Nevertheless, Milnor numbers are perfectly well defined for string links and, actually, their undeterminacy for links corresponds exactly to the undeterminacy which arises when cutting open links into string links. In [HL90], N. Habegger and X-S. Lin showed that every string link is link-homotopic to a pure braid, and that the latter are classified, still up to link-homotopy, by non repeating Milnor numbers. But, though equivalent to the knowledge of all non repeating Milnor numbers, Habbeger–Li's invariant take the form of a *basis-conjugating automorphisms* of the reduced free group RF_n, generalizing hence the Artin representation point of view on the braid group [Art47].

As for links, string links can be studied through their diagrams up to Reidemeister moves. The link-homotopy can also be interpreted in this framework as the equivalence relation induced by the *self-crossing change*, the local move on diagrams which swaps the over/under information on a double point whose preimages are both on the same connected component.

From a combinatorial point of view, link and string link diagrams can be interpreted as planar 4-valent graphs and the local moves on diagrams as local moves on such decorated graphs. By relaxing the planarity constraint, one define *virtual* objects. Despite their purely diagrammatical nature, most topological invariants can be extended to the virtual setting. For instance, the *Wirtinger presentation* provides a diagrammatical way to compute the fundamental group which straightforwardly extends to virtual objects. It is remarkable that most of these combinatorial extensions of topological invariants occur to be invariant under a certain local move, called *over-commute* and denoted by OC. The *welded* knot theory is defined as the quotient of the virtual knot theory under OC. Even if this definition may look rather arbitrary, it can be

topologically legitimized within the frame of knotted surfaces as the combinatorics of higher dimensional 4–valent singularities.

The theory of knotted surfaces in dimension 4 takes its origins in the mid 20$^{\text{ies}}$, from the work of E. Artin [Art25]. However, the systematic study of these objects only really began in the early 60$^{\text{ies}}$, notably through the work of M. Kervaire, R. Fox and J. Milnor [FM66, KM61, Ker65], but also of T. Yajima or T. Yanagawa, in Japan[1]. From this early stage, one can distinguish two approaches to study surfaces. One, emerging from the higher dimensions, fits into a strongly algebraical perspective; the second, emerging from dimension 3, recycles the diagrammatical aspects of knot theory. Just as links, surfaces can indeed be generically projected on a hyperplane and studied through the decorated immersions that it generates, called *broken surface diagrams*. But the set of possible singularities is then broader: there are still double points loci, but also some triple and branch points. One can however decide to restrict his analysis to diagrams with only double points, and the corresponding combinatorics is then very close to link diagrams. In [Yaj62], T. Yajima defined indeed a procedure, so-called Tube, which inflates link diagrams into knotted tori. Another procedure, so-called Spun, gives the diagram a spin around an axis. Both yields the same well defined and injective map from links to knotted tori. Soon, the subclass of sphere diagrams with only double points, called *simple* in the literature, has been given a topological flavor when identified by T. Yanagawa [Yan69a, Yan69b, Yan70] as the *ribbon* subclass, which is the class of surfaces which bound immersed 3-dimensional spaces whose singular sets contain only a certain type of *ribbon singularities*. For tori, the ribbon class is strictly smaller than the simple one, but the images of the Tube map are actually ribbon. Of course, the classical link theory corresponds only to some ribbon tori, but in 2000, S. Satoh [Sat00] showed that—at the cost of injectivity—the Tube map can be extended into a surjective map from welded links to ribbon tori.

The Tube map is hence a bridge between the welded theory—which can be seen as an extension of the classical link theory—and the ribbon theory—which can be seen as a midstep toward general knotted surfaces theory. The work presented here builds on this bridge to generalize Habbeger–Lin classification to dimension 4. We introduce *string* 2*–links*, which are annuli properly embedded in B^4 with unlinked and unknotted boundaries fixed in $\partial B^4 \cong S^3$, and classify them up to link-homotopy. There are three steps in the proof. First, we prove the statement for the ribbon subclass up to an *a priori* restricted notion of ribbon link-homotopy. Second, we prove that the ribbon subclass is generic up to link-homotopy, in the sense that every string 2–link is link-homotopic to a ribbon one. Finally, we prove that the classifying invariant in the ribbon case is actually invariant under general link-homotopy.

For the first step, we start by reducing classical string links to the data, for a given diagram, of the interconnections between its double points seen as 4-valent singularities. Using a coloring by RF_n elements process on this combinatorial substratum, we provide an alternative definition of Habbeger–Lin's invariant, and this definition straightforwardly extends to the welded case, and hence to the ribbon one. Actually, we take the opportunity of this dissertation to handle, in all generality, the ribbon codimension two case in any higher dimension.

The next two steps strongly rely on broken surface diagrams, but link-homotopy raises then a new problem. Indeed, in dimension 3, singular string links can be generically desingularized by infinitesimal perturbation, so that link-homotopy reduces to a local move on diagrams. But in dimension 4, a singular surface has generically a finite number of singular points which cannot be locally removed. Consequently, we first develop a broken surface diagram theory for immersed surfaces, and we give three singular moves which, together with *Roseman moves* from the embedded case, generates link-homotopy. At the same time, we provide sets of moves generating respectively, ambient isotopy for singular surfaces, regular homotopy and general homotopy. Using these singular broken surface diagrams, and again with a coloring by RF_n elements process, we extend Habbeger–Lin's invariant to any string 2–link, and prove that it is invariant under link-homotopy. Finally, we show that the above-mentioned genericity result for the ribbon subclass up link-homotopy, is equivalent to a theorem by A. Bartels et P. Teichner stating that embedded spheres in S^4 are always link-homotopically trivial [BT99].

Compared with Habbeger–Lin and J. Milnor's works, Bartels–Teichner's theorem sems to suggest a real

[1] see below for references or [Suz76] for a complete bibliography

break between dimensions 3 and 4. It does not. The links and string links classifications crystallize indeed on the notion of longitudes; but as spheres are simply connected, there is no such longitude for them. It is hence more natural that the classification extends to knotted tori better than to spheres. This is, at least, the philosophy underlying the first part of the present dissertation.

Notation and setting

Once for all, we set a non negative integer n, and we let I be the closed interval $[0,1]$.

We begin with some topological notation and setting. We fix n distinct points $\{\tilde{p}_i\}_{i\in\{1,\dots,n\}}$ in $\mathring{B}^1 = (-1,1)$, say *e.g.* $\tilde{p}_i = \frac{2i-n-1}{n+1}$. Then we choose disjoint discs $D_1,\dots,D_n$ in the interior of the 3–ball $B^3 \cong B^2\times B^1$ such that $p_i := (0,\tilde{p}_i) \in \mathring{D}_i$ for every $i\in\{1,\dots,n\}$, say *e.g.* $D_i = \left\{(0,y,z)\in B^2\times I \mid y^2+(z-\tilde{p}_i)^2 \leq \frac{1}{2(n+1)^2}\right\}$. We denote by $C_i := \partial D_i$ the oriented boundary of D_i. More generally, for every positive integer $d\geq 2$, we shall choose disjoint d–dimensional balls $D_1^d,\dots,D_n^d$ in the interior of $B^{d+1}\cong B^d\times B^1$ such that $p_i^d := (0,\tilde{p}_i)\in \mathring{D}_i^d$ for every $i\in\{1,\dots,n\}$. We denote by $C_i^{d-1} := \partial D_i^d$ the oriented boundary of D_i^d.

We will also consider the d–ball seen as $B^d\cong B^{d-1}\times I$, we shall then set $\partial_0 B^d := B^{d-1}\times\{0\}$, $\partial_1 B^d := B^{d-1}\times\{1\}$ and $\overset{*}{B}{}^d := \mathring{B}^d \cup (\partial_0\mathring{B}^d)\cup(\partial_1\mathring{B}^d)$. By an *embedded* (resp. *immersed*) *submanifold* $X\subset B^d$, we shall mean the image of a smooth embedding (resp. immersion) $f_X : \tilde{X}\to B^d$ of a manifold $\tilde{X}$, called the underlying *abstract manifold*, into B^d such that

- $X\subset \overset{*}{B}{}^d$;
- $X\cap\left(B^{d-1}\times[0,\varepsilon)\right) = \left(X\cap\partial_0 B^d\right)\times[0,\varepsilon)$ and $X\cap\left(B^{d-1}\times(1-\varepsilon,1]\right) = \left(X\cap\partial_1 B^d\right)\times(1-\varepsilon,1]$ for some $\varepsilon>0$.

For a *proper* embedded (resp. immersed) submanifold, we shall moreover assume that $\partial X := f(\partial\tilde{X}) = X\cap(\partial_0 B^d\cup\partial_1 B^d)$. An immersion shall be called a *self-immersion* if, for every $x\in X$, $f^{-1}(x)$ is contained in a connected component of $\tilde{X}$. In all cases, we set:

- $\partial_0 X = X\cap\partial_0 B^d$, the *lower boundary* of X;
- $\partial_1 X = X\cap\partial_1 B^d$, the *upper boundary* of X;
- $\partial_* X = \partial X\setminus(\partial_0\mathring{X}\sqcup\partial_1\mathring{X})$, the *lateral boundary* of X;
- $\partial_*\tilde{X}$ the preimage of $\partial_* X$ in $\tilde{X}$;
- $\overset{*}{X} = X\setminus\partial_* X$.

By a *tubular neighborhood* of X in B^d, we shall mean an open set N such that $N\cap\mathring{B}^d$ is a tubular neighborhood of $\mathring{X}$ in $\mathring{B}^d$ and $\partial_\varepsilon N$ is a tubular neighborhood of $\partial_\varepsilon X$ in $\partial_\varepsilon B^d$ for $\varepsilon\in\{0,1\}$. All the isotopies considered in this dissertation shall be assumed to be smooth and to fix the lower and upper boundaries.

If $X_1, X_2\subset B^d$ are two embedded or immersed submanifolds[2] such that $\partial_1 X_1 = \partial_0 X_2$, then we define $X_1\bullet X_2$, the *stacking product* of X_1 and X_2, as the image of $f_{X_1\bullet X_2}\colon \tilde{X}_1\cup\tilde{X}_2/_\sim \longrightarrow B^d$ where $x_1\sim x_2$ iff

- $x_1\in\tilde{X}_1$ and $x_2\in\tilde{X}_2$;
- $f_{X_1}(x_1)\in\partial_1 X_1$ and $f_{X_2}(x_2)\in\partial_0 X_2$;
- $(\pi\circ f_{X_1})(x_1) = (\pi\circ f_{X_2})(x_2)$ where $\pi\colon B^{d-1}\times I\longrightarrow B^{d-1}$ is the first projection;

and

$$f_{X_1\bullet X_2}(x) = \begin{cases} (y,\frac{t}{2}) \text{ if } x\in\tilde{X}_1 \text{ and } f_{X_1}(x) = (y,t)\in B^{d-1}\times I \\ (y,\frac{1+t}{2}) \text{ if } x\in\tilde{X}_2 \text{ and } f_{X_2}(x) = (y,t)\in B^{d-1}\times I \end{cases}.$$

Throughout this paper, and for various types of objects, diagrammatical or topological, we will consider local moves. A *local move* is a transformation that changes the object only inside a ball of the appropriate dimension. By convention, it will be represented by the full content of the ball where the move occurs, and the reader should keep in mind that there is a non represented part, which is identical for each side of the move.

[2] possibly endowed with further local datas such as arrows or over/under information at double points

We also define some algebraic notation. For any group G, we denote by

- $a^b := b^{-1}ab$ the conjugate of a by b for every $a, b \in G$;
- $[a;b] := a^{-1}b^{-1}ab$ the commutator of a and b for every $a, b \in G$;
- $\Gamma_k G$, for $k \in \mathbb{N}^*$, the k^{th} term of the lower central series of G inductively defined by $\Gamma_1 G = G$ and $\Gamma_{k+1}G := \left[G; \Gamma_k G\right]$;

and, if G is normally generated by elements $g_1, \dots, g_p$, we further denote by

- $RG := {}^{G}\!/\!\left\{[g_i; g_i^g] \,\middle|\, i \in \{1, \dots, p\}, g \in G\right\}$ the *reduced quotient of* G, which is the smallest quotient where each generator commutes with all its conjugates;
- $\mathrm{End}_{\mathrm{C}}(G) := \left\{f \in \mathrm{End}(G) \,\middle|\, \forall i \in \{1, \dots, p\}, \exists g \in G, f(g_i) = g_i^g\right\}$, the monoid of *basis-conjugating endomorphisms* of G, and $\mathrm{Aut}_{\mathrm{C}}(G) \subset \mathrm{End}_{\mathrm{C}}(G)$ the subgroup of its inversible elements.

We shall denote by F_n the free group on n generators; unless otherwise specified, generators of F_n will be denoted by $x_1, \dots, x_n$. By abuse of notation, and since it shall not introduce any ambiguity, the same notation shall be used to denote an element and its image under a given quotient. Similarly, names of map may be kept when considering their induced counterpart under a given quotient.

Finally, we recall that a *poset* is a set E given with a partial order $\leq_E$ characterized by some subset $\Omega_{\leq_E} \subset E \times E$. Two elements $x, y \in E$ are said *comparable* if either $x \leq_E y$ or $y \leq_E x$. The poset E has a *total order* if any two elements of E are comparable. Whenever they exist, for instance when E is a finite totally ordered poset, we define

- $\max(E)$ and $\min(E)$ the unique elements which are, respectively, greater and smaller to any other element of E;
- the *closest predecessor of* $x \in E$, which is $\max\left(\left\{y \in E \mid y <_E x\right\}\right)$;
- the *closest successor of* $x \in E$, which is $\min\left(\left\{y \in E \mid x <_E y\right\}\right)$.

We say that a poset E' *extends* E iff $E' = E$ as sets and $\Omega_{\leq_E} \subset \Omega_{\leq_{E'}}$, that is iff $x \leq_{E'} y$ whenever $x \leq_E y$.

1 Classification of classical string links up to link-homotopy

As a warm up, we begin by reviewing Habegger and Lin's classification of string links up to link-homotopy, as given in [HL90].

1.1 String links

Definition 1.1. A *string link* is a proper embedding $\bigsqcup_{i \in \{1,\dots,n\}} I_i$ of n disjoint and oriented copies of I in $B^3 \cong B^2 \times I$ such that, for every $i \in \{1, \dots, n\}$ and $\varepsilon \in \{0, 1\}$, $\partial_\varepsilon I_i = \left((0, \tilde{p}_i), \varepsilon\right)$, and I_i is oriented from $\partial_0 I_i$ to $\partial_1 I_i$. We denote by SL_n the set of string links up to isotopy. It is naturally endowed with a monoidal structure by the stacking product.

Example 1.2. *Pure braids* can be seen as the special case of string links which stay transverse to the foliation $\sqcup_{t \in I} B^2 \times \{t\}$. They actually corresponds to inversible elements in SL_n, see [HM12, Kre14].

For every string link L, we shall define its *fundamental group* $\pi_1(L)$ as the fundamental group of the complement of a tubular neighborhood of L in B^3. For every $i \in \{1, \dots, n\}$, the i^{th} *bottom* and *top meridians* of L are defined as the loops $m_0, m_1 \in \pi_1(L)$, which enlace positively p_i in, respectively, $\partial_0 X_L$ and $\partial_1 X_L$. A i^{th} *longitude* for L is any path on the boundary of the tubular neigborhood of the i^{th} interval component of L which runs from $\partial_1 X_L$ to $\partial_0 X_L$, closed by a standard path on ∂B^3. It can be noted that any two i^{th} longitudes differ from a post-composition with a power of the i^{th} bottom meridian.

Definition 1.3. A *self-singular string link* is a self-immersion $\bigsqcup_{i \in \{1,\dots,n\}} I_i$ of n disjoint copies of the oriented interval I in B^3 satisfying the same boundary conditions than regular string links.

Two string links are said *link-homotopic* if there is a smooth path of self-singular string links[3] connecting them. We denote by SL_n^{lh} the quotient of SL_n under link-homotopy.

[3] note that, by definition, a string link is a self-singular string link

Proposition 1.4 ([HL90])**.** *Any string link is link-homotopic to a pure braid.*

Corollary 1.5. *The monoid SL^{lh}_n is a group.*

1.2 Reduced peripheral systems

It is well known that classical links are classified by their peripheral systems, that is by their fundamental group given with meridians and longitudes; see *e.g.* [Hem76] for a detailled proof. Non repeating Milnor's invariants, in one hand, and Habegger and Lin's Artin–like invariant can be seen as two perspectives on some kind of reduced peripheral system notion. In the case of string links, and later in the case of string d–links, we shall see that the reduced fundamental group is always RF_n, where generators can conventionally be choosen as, say, the bottom meridians. It follows that, for a reduced peripheral system, only longitudes do matter and, though, only up to a power of the corresponding meridians. This motivates the following definitions.

Definition 1.6. A *reduced peripheral system* is an n–uple $(\lambda_1, \dots, \lambda_n) \in \prod_{i=1}^n \mathrm{RF}^{(i)}_{n-1}$, where $\mathrm{RF}^{(i)}_{n-1} \subset \mathrm{RF}_n$ is the subgroup generated by all the generators $x_1, \dots, x_n$ but x_i.

To a reduced peripheral system $\Lambda := (\lambda_1, \dots, \lambda_n)$, one can associate a basis-conjugating endomorphism $\varphi_\Lambda \in \mathrm{End_C}(\mathrm{RF}_n)$ defined, for every $i \in \{1, \dots, n\}$, by $\varphi_\Lambda(x_i) = x_i^{\lambda_i}$. Reciprocally, we proved the following:

Lemma 1.7 ([8, Lem. 4.25])**.** *For every $\varphi \in End_C(RF_n)$, there a unique reduced peripheral system Λ such that $\varphi_\Lambda = \varphi$.*

To a reduced peripheral system $\Lambda := (\lambda_1, \dots, \lambda_n)$, one can also associate Milnor numbers defined as follows. For each $i \in \{1, \cdots, n\}$, we denote by $\mathcal{S}^{(i)}_{n-1} := \mathbb{Z}\langle\langle X_1, \cdots, \hat{X}_i, \cdots, X_n\rangle\rangle$ the ring of formal power series in $(n-1)$ non-commutative variables denoted by $X_1, \dots, X_n$ with X_i removed. By $E_i : \mathrm{F}^i_{n-1} \to \mathcal{S}^{(i)}_{n-1}$ we denote the Magnus expansion, which is the group homomorphism sending the j^{th} generator to $1 + X_j$; it descends to a well defined homomorphism E^r_i from $\mathrm{RF}^{(i)}_{n-1}$ to $\mathcal{S}^{(i)}_{n-1}/I_r$, where I_r is the ideal generated by monomials with repetitions. It is known since Magnus, see [MKS04], that E_i is injective, and this remains true for its reduced counterpart:

Lemma 1.8 (*e.g.* [Yur08])**.** *The maps E^r_i are injective.*

For every sequence $I = i_1 \cdots i_k i$ of pairwise distinct integers in $\{1, \dots, n\}$, we define $\mu_I(\Lambda)$, the *Milnor invariant of index I* for Λ, as the coefficient of the monomial $X_{i_1} \cdots X_{i_k}$ in $E^r_i(\lambda_i)$. These Milnor invariants are said *non repeating* since we only consider here sequences of distinct integers. It follows from Lemma 1.8 that Λ can be recovered from the set of all its non repeating Milnor invariants.

Corollary 1.9. *The data of a reduced peripheral system, of its associated basis-conjugating endomorphism, or of its associated non repeating Milnor invariants are all equivalent.*

This statement being set, we shall now focus on the basis-conjugating endomorphism point of view.

1.3 Habegger and Lin's Artin–like invariant

Let L be a string link and denote by X_L the complement of a tubular neighborhood of L in B^3. Both $\partial_0 X_L$ and $\partial_1 X_L$ are n–punctured discs and the inclusion maps $\iota_\varepsilon \colon \partial_\varepsilon X_L \longrightarrow X_L$, for $\varepsilon \in \{0, 1\}$, induce maps at the π_1–level. It is easily seen that they also induce isomorphisms at the H_1 and H_2–level. All the conditions are hence met to apply the following theorem of J. Stallings:

Theorem 1.10 ([Sta65])**.** *If a map $\iota \colon X \longrightarrow Y$ induces an isomorphism at the H_1–level and an epimorphism at the H_2–level then, for every $k \in \mathbb{N}^*$, it induces an isomorphism between $\pi_1(X)/\Gamma_k\pi_1(X)$ and $\pi_1(Y)/\Gamma_k\pi_1(Y)$.*

But the fundamental group of a punctured disc is easily computed to be the free group generated by the meridians around each puncture; it follows that $\pi_1(\partial_0 X_L)$ and $\pi_1(\partial_1 X_L)$ can be seen as F_n generated by, respectively, the bottom and the top meridians of L. On the other hand, $\pi_1(X_L)$ can be given a Wirtinger presentation showing that it is normally generated by either the bottom or by the top meridians of L. Building on Stallings' theorem, Habegger and Lin obtain the following:

Lemma 1.11 ([HL90]). *The maps $\iota_0, \iota_1 : RF_n \longrightarrow R\pi_1(X_L)$ are both group isomorphisms.*

They can hence define the map $\varphi_L := \iota_0^{-1} \circ \iota_1 \in \mathrm{Aut}(\mathrm{RF}_n)$ which actually conjugates the i^{th} generator of RF_n, seen as $R\pi_1(X_L)$ generated by the bottom meridians, by the reduced image of any i^{th} longitude. This can also be interpreted as expresing the top meridians in terms of the bottom ones. In particular, φ_L sends every generator of RF_n to a conjugate of itself, and it is easily seen that it sends the loop that enlaces all the punctures in $\partial_1 X_L$ to itself; φ_L is hence an element of $\mathrm{Aut}^0_{\mathrm{C}}(\mathrm{RF}_n) := \left\{\varphi \in \mathrm{Aut}_{\mathrm{C}}(\mathrm{RF}_n) \mid \varphi(x_1 x_2 \cdots x_n) = x_1 x_2 \cdots x_n\right\}$.

Proposition 1.12 ([HL90]). *The map $\varphi_L \in Aut^0_C(RF_n)$ is invariant under link-homotopy.*

Theorem 1.13 ([HL90]). *The map Art:* $\left\{\begin{array}{ccc} SL_n^{lh} & \longrightarrow & Aut^0_C \\ L & \longmapsto & \varphi_L \end{array}\right.$ *is a group isomorphism.*

2 Classification of welded string links up to self-virtualization

In this section, we shall focus on the welded knot theory. It is a quotient of the virtual knot theory, which is itself a combinatorial extension of the classical knot theory seen from the diagram point of view. Knot diagrams can indeed been interpreted as planar quadrivalent oriented graphs whose vertices are decorated with some over/under information. For virtual diagrams, the planarity condition is released, and this provide a tool to describe links in thickened surfaces up to handle stabilizations, see [Kup03]. Welded diagrams are, in turn, a quotient of virtual diagrams, particularly adapted to the study of ribbon surfaces in B^4, and more generally to ribbon codimension two subspaces in higher dimensions. In all these situations, welded diagrams can be thought of as a combinatorial description of the connexions between some four-ended singularities. Hereinafter, we shall accordingly adopt an approach in compliance with this idea.

2.1 Welded knot theory

As an attempt to extract the very combinatorial essence of welded knot theory, we shall start by a purely combinatorial definition, that we will develop then into its two, more standard, realizations: Gauss and welded diagrams. Section 2.1.2 is hence likely to enlighten the definitions of Section 2.1.1, and the reader is invited to travel back and forth between these two sections. In this welded setting, we will finally define a self-virtualization theory that shall combinatorially mimic link-homotopy.

2.1.1 Welded systems

Definition 2.1. A *welded system* is a finite poset $W =: \overline{W} \sqcup \{1, \ldots, n\}$ given with a map

$$\begin{array}{ccc} \overline{W} & \longrightarrow & W \times \{\pm 1\} \\ a & \longmapsto & \big(t_W(a), \sigma_W(a)\big) \end{array}$$

such that

- for every $a \in W$, there is a unique $i \in \{1, \ldots, n\}$ such that $i \leq a$;
- for every $i \in \{1, \ldots, n\}$, $W_i := \left\{a \in W \mid i \leq a\right\}$ is totally ordered.

In other words, W is a disjoint union of n totally ordered finite sets $(W_i)_{i \in \{1,\ldots,n\}}$, indexed by their minimal elements which are chosen to be the elements of $\{1, \ldots, n\}$.

Two welded systems W_1 and W_2 are *equivalent* if there is a poset bijection $\xi : \overline{W}_2 \longrightarrow \overline{W}_1$ which satisfies, when extended by the identity on $\{1, \ldots, n\}$, $t_{W_2} = \xi \circ t_{W_1} \circ \xi^{-1}$ and $\sigma_{W_2} = \sigma_{W_1} \circ \xi$.

Elements of $\overline{W}$ are called *arrows*, and we morever say that $a \in \overline{W}$ is a *self-arrow* if a and $t_W(a)$ are comparable, that is if they belong to the same W_i. We say that a welded system W is

- *horizontal* if it has no self-arrow and if there is a second order $\leq_g$ on W which is global and extends $\leq_W$ in such a way that, for every $a \in \overline{W}$, $t_W(a) = \max\left(\left\{b \in W_{i_a} \mid b \leq_g a\right\}\right)$ where $i_a \in \{1, \dots, n\}$ is the index such that $t_W(a) \in W_{i_a}$;
- *ascendant* if $\mathrm{Im}(t_W) \subset \{1, \dots, n\}$.

For every welded system W, we set $\mathrm{pre}\colon \overline{W} \longrightarrow W$, the map which sends any element of $\overline{W}$ to its closest predecessor. We shall now define three local moves on welded systems:

R1: let W be a welded system which contains an element $a \in \overline{W}$ such that $t_W(a)$ is either a or $\mathrm{pre}(a)$, then applying R1 to W with regard to a leads to the welded system W_a which is equal to $W \setminus \{a\}$ as a poset, with $\sigma_{W_a} := (\sigma_W)_{|W_a}$ and $t_{W_a} := (\pi_a \circ t_W)_{|W_a}$, where $\pi_a\colon W \longrightarrow W_a$ is the identidy map except on a which is sent to $\mathrm{pre}(a)$;

R2: let W be a welded system which contains two elements $a_1, a_2 \in \overline{W}$ such that $\mathrm{pre}(a_1) = a_2$, $t_W(a_1) = t_W(a_2)$, $\sigma_W(a_1) = -\sigma_W(a_2)$ and $t_W^{-1}(a_2) = \emptyset$, then applying R2 to W with regard to a_1 and a_2 leads to the welded system W_{a_1,a_2} which is equal to $W \setminus \{a_1, a_2\}$ as a poset, with $\sigma_{W_{a_1,a_2}} := (\sigma_W)_{|W_{a_1,a_2}}$ and $t_{W_{a_1,a_2}} := (\pi_{a_1,a_2} \circ t_W)_{|W_{a_1,a_2}}$, where $\pi_{a_1,a_2}\colon W \longrightarrow W_{a_1,a_2}$ is the identidy map except on a_1 and a_2 which are both sent to $\mathrm{pre}(a_2)$;

R3: let W be a welded system which contains three elements $a_1, a_2, a_3 \in \overline{W}$ such that $\mathrm{pre}(a_2) = a_3$, $t_W(a_2) = t_W(a_3)$, $\sigma_W(a_2) = -\sigma_W(a_3)$ and $t_W^{-1}(a_3) = \{a_1\}$, then applying R3 to W with regard to a_1, a_2 and a_3 leads to the welded system W_{a_1,a_2,a_3} which is equal to W as a set, whose partial order is such that it coincides with that of W on $W \setminus \{a_2, a_3\}$ but satisfies $\mathrm{pre}(a_3) = a_1$ and $\mathrm{pre}(a_1) = a_2$, and with $\sigma_{W_{a_1,a_2,a_3}} := \sigma_W$ and $t_{W_{a_1,a_2,a_3}} := \pi_{a_1,a_2,a_3} \circ t_W$, where $\pi_{a_1,a_2,a_3}\colon W \longrightarrow W_{a_1,a_2,a_3}$ is the identidy map except on a_1 which is sent to a_3, and on a_2 and a_3 which are both sent to $\mathrm{pre}(a_3)$.

For two welded systems W_1 and W_2, we finally define the product $W_1 \bullet W_2$ as the welded system defined by $W_1 \underset{\{1,\dots,n\}}{<} \overline{W}_2$, that is by $W_1 \sqcup \overline{W}_2$ where two elements x_1 and x_2 satisfy $x \leq_{W_1 \bullet W_2} y$ iff either $x_1, x_2 \in W_i$ and $x_1 \leq_{W_i} x_2$ for some $i \in \{1, 2\}$, or $x_1 \in W_1$, $x_2 \in W_2$ and there is some $i \in \{1, \dots, n\}$ such that $i \leq_{W_1} x_1$ and $i \leq_{W_2} x_2$. The map $\sigma_{W_1 \bullet W_2}$ is then σ_{W_i} on $\overline{W}_i$, for both $i \in \{0, 1\}$, and $t_{W_1 \bullet W_2}$ is t_{W_1} on $\overline{W}_1$ and $\pi_{W_1} \circ t_{W_2}$ on $\overline{W}_2$, where $\pi_{W_1}\colon W_2 \longrightarrow W_1 \sqcup \overline{W}_2$ is the identity map on $\overline{W}_2$ and sends $i \in \{1, \dots, n\}$ to $\max\left\{x \in W_1 \mid i \leq x\right\}$.

Definition 2.2. We define $w\mathrm{SL}_n$, the set of *welded string links*, as the quotient of welded systems under equivalence and moves R1, R2 and R3. It is endowed with a monoidal structure by the $\bullet$ product, with unit $\mathbb{1} := \{1, \dots, n\} \sqcup \emptyset$.

It can already be noticed that horizontal welded systems are invertible in $w\mathrm{SL}_n$. Indeed, let W be such a welded system given with a global order $\leq_g$; then one can define W^{-1} as the set W with

- reversed partial order, defined by $a_1 \leq_{W^{-1}} a_2$ iff $a_2 \leq_W a_1$;
- $\sigma_{W^{-1}}(a) = -\sigma_W(a)$;
- $t_{W^{-1}}(a) = \begin{cases} i \text{ if } t_W(a) = \max(W_i) \\ \text{the closest successor of } t_W(a) \text{ otherwise.} \end{cases}$.

Using R2 on $W \bullet W^{-1}$, one can inductively remove by pair the maximal element, according to $\leq_g$, of W with its counterpart in W^{-1}, until ending eventually with $\mathbb{1}$.

2.1.2 Two diagrammatic realizations of welded systems

We present now two standard ways to picture welded systems. As a matter of fact, every reference that we shall provide for proofs on welded systems will actually deal with either Gauss or welded diagrams; nonetheless, they will always adapt to the welded systems case, sometime in an even smoother way.

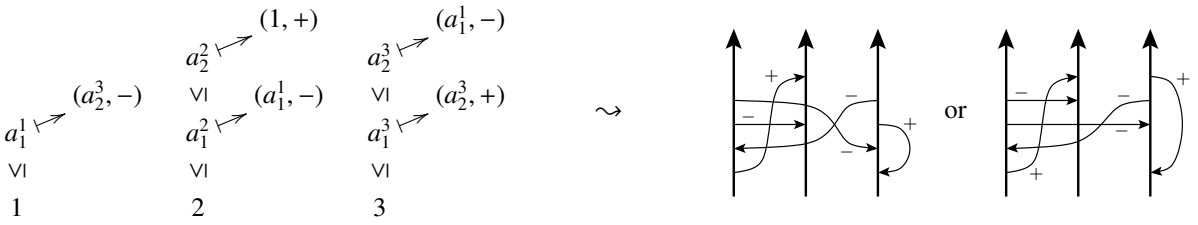


Figure I.1: From welded systems to Gauss diagrams

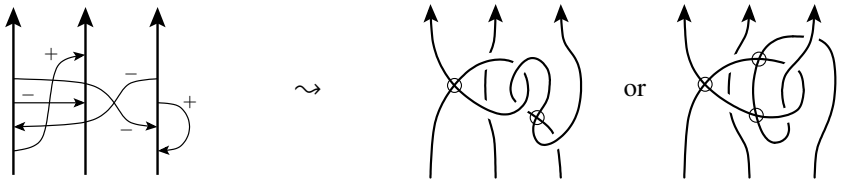


Figure I.2: From Gauss diagrams to welded diagrams

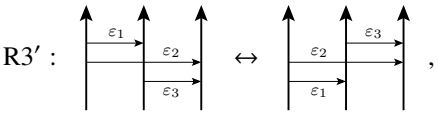
Gauss diagrams

A welded system W can be represented by a *Gauss diagram*—introduced in [PV94], see also [GPV00, Fie01]—as follows. First draw n vertical strands, one for each $i \in \{1,\dots,n\}$. For every $i \in \{1,\dots,n\}$, represent each element of W_i by a point of the i^{th} strand such that i is the bottom end of the strand, and the other points are ordered on the strand as prescribed by the order on W_i. For every $a \in W \setminus \{1,\dots,n\}$, draw an arrow which points to a and starts from the portion of strand which is just above $t_W(a)$ and label it by $\sigma_W(a)$. See Figure I.1 for examples. To get an actual Gauss diagram, one should be watchful that none of the arrow tails do coincide. One make then some arbitrary but meaningless choices; as a matter of fact, Gauss diagrams should be considered up to the local OC move, shown in the lower left corner of Figure I.3.

It can be noted that the welded systems terminology is largely inspired by Gauss diagram representation. For instance:

- arrows in welded systems corresponds to actual arrows in Gauss diagrams, or more precisely to their heads; and self-arrows to arrows with both ends on the same strand;
- horizontal welded systems correspond to welded systems which can be represented by a Gauss diagram with only horizontal arrows;
- ascendant ones correspond to welded systems which can be represented by a Gauss diagrams whose arrows are all going from the lower halves to the upper halves of the strands.

Welded string links can be thought of as Gauss diagrams up to OC, R1, R2 and R3 moves shown in Figure I.3. Up to OC moves, there is actually a one-to-one correspondence between eponymous moves for welded systems and Gauss diagrams. Note however that, in the literature, R3 for Gauss diagram is more standardly defined as:



with some sign restrictions on ε_1, ε_2 and ε_3. But for Gauss diagrams up to OC and R2 moves, R3 and R3′ are equivalent and, as highlighted by the work of J-B. Meilhan and A. Yasuhara in [MY17], the former appears

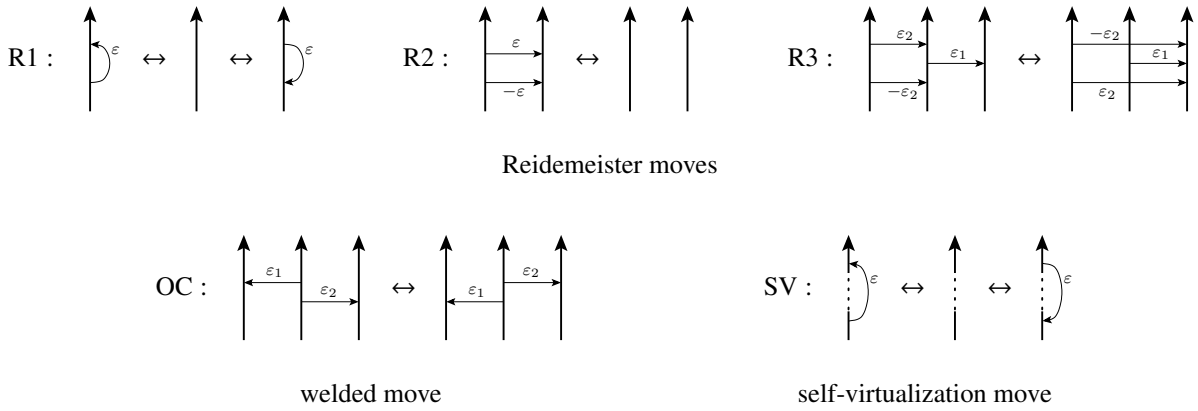


Figure I.3: Local moves on Gauss diagrams:
here, $\varepsilon, \varepsilon_1, \varepsilon_2 \in \{\pm 1\}$, vertical lines are portions of strand that may or may not be otherwise connected, dotted lines mean that the portions are indeed connected

to be more natural from a combinatorial perspective. We should nonetheless mention that this equivalence is not anymore true for virtual objects. From the Gauss diagram point of view, the $\bullet$ product is nothing but the stacking product, and the unit element the Gauss diagram with no arrow.

Welded diagrams

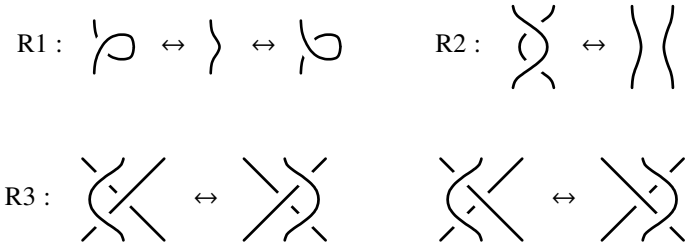
A Gauss diagram G can, in turn, be represented by a *welded diagram* as follows. In the interior of $B^2 \cong B^1 \times I$, draw one positive crossing for each $(+1)$–labeled arrow of G, and one negative crossing for each (-1)–labeled arrow. Each crossing is hence oriented, corresponds to an arrow a and has four ends:

- the pointing out (resp. in) end of the overstrand, that shall correspond to the portion of strand just above (resp. below) the head of a;
- the pointing out (resp. in) end of the understrand, that shall correspond to the portion of strand just above (resp. below) the tail of a.

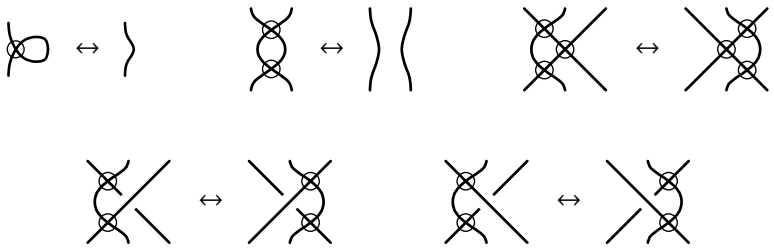
Now, for each $i \in \{1, \dots, n\}$, draw a line—that we shall call *strand*—which starts at $(\tilde{p}_i, 0)$, passes through the crossings as prescribed by how arrow ends are met when running the i^{th} strand of G from bottom to top, and ends at $(\tilde{p}_i, 1)$. Doing so, one may have to add some additional crossing; these crossings shall be called *virtual* and represented by circled crossings. See Figure I.2 for examples. When drawing these strands, some arbitrary but meaningless choices are made; as a matter of fact, welded diagrams should be considered up to the virtual moves shown in the central part of Figure I.4. Moreover, since Gauss diagrams are considered up to OC moves, welded diagrams should also be considered up to the *welded move*, shown in the lower left corner of Figure I.4.

Horizontal welded systems correspond to welded systems which can be represented by a monotonic welded diagram, in the sense that the strands are all transverse to the foliation $\sqcup_{t \in I} I \times \{t\}$. It actually corresponds to what is commonly called *welded pure braids*.

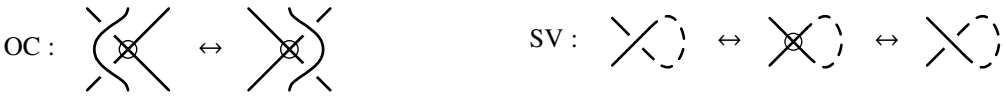
Welded string links can be thought of as welded diagrams up to R1, R2, R3, OC and virtual moves, shown in Figure I.4. Again, up to OC and virtual moves, there is a one-to-one correspondence between eponymous R1 and R2 moves for welded systems/Gauss diagrams and welded diagrams. To extend the



Reidemeister moves



virtual moves

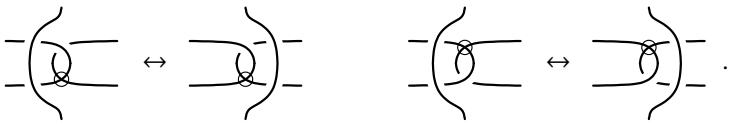


welded move

self-virtualization move

Figure I.4: Local moves on welded diagrams:
dotted lines mean that the portions of strand are belonging to the same strand

correspondence, we should have replaced R3 by the moves



But to maintain the filiation with the classical knot theory more visible, we kept the standard (and equivalent up to OC and R2 moves) R3 move. From the welded diagram point of view, the $\bullet$ product is also nothing but the stacking product, and the unit element the welded diagram with n parallel strands and no crossing.

Diagrams of classical string links can be seen as welded diagrams with no virtual crossing. And since Reidmeister moves are part of the local moves considered to define welded string links, there is a well defined map from classical to welded string links. Using the classification of classical string links by their peripheral system, one can show that this map is actually an embedding, so that the welded knot theory can be seen as an extension of the classical knot theory. It is however a very difficult question to determine whether a given welded diagram corresponds to a classical string link or not.

2.1.3 Self-virtualization

We define now a fourth local move on welded systems:

SV: let W be a welded system which contains a self-arrow $a \in \overline{W}$, then applying SV to W with regard to a leads to the welded system W_a which is equal to $W \setminus \{a\}$ as a poset, with $\sigma_{W_a} := (\sigma_W)_{|W_a}$ and $t_{W_a} := (\pi_h \circ t_W)_{|W_a}$, where $\pi_a \colon W \longrightarrow W_a$ is the identidy map except on a which is sent to $\mathrm{pre}(a)$.

Definition 2.3. Two welded systems are said *SV–equivalent* if they are connected by a finite sequence of moves R1, R2, R3 and SV moves. We denote by $w\mathrm{SL}_n^{sv}$ the monoid of welded string links up to SV–equivalency.

When thought of as Gauss or welded diagrams, SV–equivalent classes of welded string links can be understood as the quotient under the eponymous SV move, shown in the lower right corners of Figures I.3 and I.4

Proposition 2.4 ([8, Th. 4.12])**.** *Every welded system is SV–equivalent to an horizontal welded system.*

Corollary 2.5. *The monoid wSL_n^{sv} is a group.*

These two propositions, which are proven in a combinatorial way, should be compared with Proposition 1.4 and Corollary 1.5. We end this section with the following "Proposition 2.4"–like lemma which has no counterpart in Habegger and Lin's approach but will have a key role in the coming classification.

Lemma 2.6 ([8, Lem. 4.16])**.** *Every welded system is SV–equivalent to an ascendant welded system.*

2.2 Classification up to self-virtualization

We give now a complete classification of welded string links up to self-virtualization which actually extends Habegger and Lin's classification.

2.2.1 Welded Artin–like invariant

Definition 2.7. Let $y_1, \dots, y_n \in \mathrm{RF}_n$. A $(y_1, \dots, y_n)$–*coloring* for a welded system W is a map $\nu \colon W \longrightarrow \mathrm{RF}_n$ such that:

- $\nu(i) = y_i$ for every $i \in \{1, \dots, n\}$;
- $\nu(a) = \nu\big(\mathrm{pre}(a)\big)^{\nu\left(t_W(a)\right)^{\sigma_W(a)}}$ for every $a \in \overline{W}$.

For every $(y_1, \dots, y_n)$–coloring ν and each $i \in \{1, \dots, n\}$, we also define $\nu^i := \nu\big(\max(W_i)\big)$.

Remark 2.8. From the welded diagram point of view, a $(y_1,\dots,y_n)$–coloring ν is nothing but a map from the set of overstrands to RF_n which has fixed images for the bottom ends and satisfies Wirtinger relation at each crossing; in other words ν can be understood as a well defined group homomorphism from the Wirtinger group of the welded diagram to RF_n, which sends the i^{th} bottom meridian to y_i. Elements $\nu^1,\dots,\nu^n$ are then the images of the top meridians.

Lemma 2.9 ([8, Lem. 4.20])**.** *Let $y_1,\dots,y_n \in RF_n$. If W_1 and W_2 are two welded systems which differ from a R1, R2, R3 or SV move, then there is a one-to-one correspondence*

$$\vartheta\colon \left\{(y_1,\dots,y_n)\text{–coloring of } W_1\right\} \longrightarrow \left\{(y_1,\dots,y_n)\text{–coloring of } W_2\right\}$$

such that $\left(\vartheta(\nu)^i\right)_{i\in\{1,\dots,n\}} = \left(\nu^i\right)_{i\in\{1,\dots,n\}}$ for every $(y_1,\dots,y_n)$–coloring ν of W_1.

It is rather obvious that an ascendant welded system admits a unique $(y_1,\dots,y_n)$–coloring. Similarly, one can observe that an horizontal welded system admits also a unique $(y_1,\dots,y_n)$–coloring. Using either Proposition 2.4 or Lemma 2.6, we obtain hence:

Proposition 2.10. *Let $y_1,\dots,y_n \in RF_n$. For every welded system W, there is a unique $(y_1,\dots,y_n)$–coloring $\nu_{(y_1,\dots,y_n)}$. In particular, there is a unique $(x_1,\dots,x_n)$–coloring ν_W of W and the elements $\left(\nu_W^i\right)_{i\in\{1,\dots,n\}}$ define invariants of welded string links up to self-virtualization.*

For every welded string link L, one can hence consider

$$\varphi_L\colon \left\{\begin{array}{ccc} \mathrm{RF}_n & \longrightarrow & \mathrm{RF}_n \\ x_i & \longmapsto & \nu_W^i \end{array}\right. ,$$

where W is any representative for L. By construction, φ_L is a basis-conjugating endomorphism of RF_n and it depends only on the SV–equivalency class of L. Moreover, by uniqueness in Proposition 2.10, we have that $\rho\circ\nu_{(x_1,\dots,x_n)} = \nu_{(\rho(x_1),\dots,\rho(x_n))}$ for any $\rho\in\mathrm{End}(\mathrm{RF}_n)$. It follows in particular that, $\varphi_{L_1\bullet L_2} = \varphi_{L_1}\circ\varphi_{L_2}$ for any two welded string links L_1 and L_2; and since $\varphi_{\mathbb{1}} = \mathrm{Id}_{\mathrm{RF}_n}$, this implies that φ_L is invertible.

Definition 2.11. We define the *welded Artin–like invariant* as the group homomorphism

$$\mathrm{Art}_w\colon \left\{\begin{array}{ccc} w\mathrm{SL}_n^{sv} & \longrightarrow & \mathrm{Aut_C}(\mathrm{RF}_n) \\ L & \longmapsto & \varphi_L \end{array}\right. .$$

2.2.2 An inverse for Art_w

Recall that, for every $i\in\{1,\dots,n\}$, $\mathrm{RF}_n^{(i)}$ is the subgroup of RF_n generated by all $x_1,\dots,x_n$ but x_i. We first consider the map $\tilde\eta\colon \prod_{i=1}^n \left\{\text{word in } \{x_1^{\pm1},\dots,x_n^{\pm1}\}\setminus\{x_i^{\pm1}\}\right\} \longrightarrow \left\{\text{ascendant welded system}\right\}$ which send $\left(x_{r_1^1}^{\varepsilon_1^1}\cdots x_{r_{k_1}^1}^{\varepsilon_{k_1}^1}\ ,\ \dots\ ,\ x_{r_1^n}^{\varepsilon_1^n}\cdots x_{r_{k_n}^n}^{\varepsilon_{k_n}^n}\right)$ to $W := \bigsqcup_{i=1}^n \left\{i\le a_1^i\le\cdots\le a_{k_i}^i\right\}$ with $t_W(a_j^i) = r_j^i$ and $\sigma_W(a_j^i) = \varepsilon_j^i$.

Lemma 2.12 ([8, Lem. 4.26])**.** *The map $\tilde\eta$ descends into a well defined map*

$$\eta\colon \prod_{i=1}^n RF_n^{(i)} \longrightarrow wSL_n^{sv}.$$

For every $\varphi\in\mathrm{Aut_C}(\mathrm{RF}_n)$, we can now use Lemma 1.7 to extract the unique reduced peripheral system $(\lambda_1,\dots,\lambda_n)\in\prod_{i=1}^n \mathrm{RF}_n^{(i)}$ such that $\varphi(x_i) = x_i^{\lambda_i}$ for every $i\in\{1,\dots,n\}$, and set $L_\varphi := \eta(\lambda_1,\dots,\lambda_n)\in w\mathrm{SL}_n^{sv}$. By construction $\mathrm{Art}_w(L_\varphi) = \varphi$; and for a welded string link L represented by an ascendant welded system, it is clear, as soon as all self-arrows has been removed using SV, that $L_{\mathrm{Art}_w(L)} = L$. It follows then from Lemma 2.6 that:

Theorem 2.13 ([8, Th. 3.11])**.** *The map $Art_w\colon wSL_n^{sv}\longrightarrow Aut_C(RF_n)$ is a group isomorphism.*

Again, this theorem should be compared with Theorem 1.13. In particular, it shows that the embedding of classical string links into welded ones induces also an embedding up to link-homotopy and self-virtualization. But more than that, it provides a very simple characterization of the classical subclass of $w\mathrm{SL}_n^{sv}$, as the automorphisms which preserve the product of all generators.

Remark 2.14. There is no reason, in general, for a basis-conjugating endomorphism to be invertible. For instance, the morphism $\varphi\colon \mathrm{F}_2 \longrightarrow \mathrm{F}_2$ which sends x_1 to $x_1^{x_2}$ and x_2 to $x_2^{x_1}$ is in $\mathrm{End_C}(\mathrm{F}_2) \setminus \mathrm{Aut_C}(\mathrm{F}_2)$. An unexpected by-product of Theorem 2.13, and more precisely of the map η, is that $\mathrm{End_C}(\mathrm{RF}_n) = \mathrm{Aut_C}(\mathrm{RF}_n)$. As a matter of fact, it is sufficient to show that $\varphi \in \mathrm{End}(\mathrm{RF}_n)$ is basis-conjugating to know that $\varphi \in \mathrm{Aut_C}(\mathrm{RF}_n)$.

3 Classification of ribbon higher dimensional string links up to ribbon link-homotopy

In this section, we define higher dimensional kind of string links, but we will right away restrict to their ribbon subclasses. Up to a certain restricted notion of link-homotopy, it will happen that their classification reduces to the classification of welded string links up to self-virtualization, whatever the dimension is. From now on, we fix hence an integer $d \geq 2$ and import all the definitions given in the Notation and setting section.

3.1 Ribbon string d–links

3.1.1 General string d–links

We start by defining the general notion of string d–links that, however, we shall study in more details only in Section 4, for the $d = 2$ case.

Definition 3.1. A *string d–link* is a proper embedding $\bigsqcup_{i\in\{1,\dots,n\}} (S^{d-1}\times I)_i$ of n disjoint copies of the thickened $(d-1)$–dimensional sphere in $B^{d+2} \cong B^{d+1}\times I$ such that, for every $i \in \{1,\dots,n\}$ and $\varepsilon \in \{0,1\}$, $\partial_\varepsilon(S^{d-1}\times I)_i = C_i^{d-1} \times \{\varepsilon\}$. We denote by d–SL_n the set of string d–links up to isotopy. It is naturally endowed with a monoidal structure by the stacking product.

Remark 3.2. In [6], string 2–links are called 2–string links. Since this terminology can already be found in the literature to denote classical string links with 2 connected components, we opted in the present dissertation for a denomination which has not been assigned yet. Not however that "string 2–links" is still contestable since, in actual fact, they are neither 2–links nor links of strings. Actually, the word "string" is irrelevant here: string 2–links should be called *annulus links*. But this terminology would have been tricky to generalize in higher dimensions. So at the end of the day, string 2–links, and more generally string d–links, occured to be the best compromise between aesthetics and convenience.

Remark 3.3. Contrary to what one might expect at first, d–SL_n does not occur to be a generalization in higher dimensions of SL_n, but of SL_{2n}. This is partly due to the fact that we will be interested in the ribbon subclass, which is well defined only for string links with an even number of strands.

We also define their singular counterparts, even if, again, we shall use them only in Section 4, for $d = 2$.

Definition 3.4. A *self-singular string d–link* is a proper self-immersion $T = \bigsqcup_{i\in\{1,\dots,n\}} (S^{d-1}\times I)_i$ of n disjoint copies of the thickened $(d-1)$–dimensional sphere S^{d-1} in $B^{d+2} \cong B^{d+1}\times I$ satisfying the same boundary conditions than regular string d–links.

Two string d–links are said *link-homotopic* if there is a smooth path of self-singular string d–links connecting them. We denote by d–SL_n^{lh} the quotient of d–SL_n under link-homotopy.

Since an embedding is a special case of immersion, regular string d–links are self-singular. However, for the sake of clarity, we shall often consider that self-singular objects are not embedded, and deal with regular objects separately.

3.1.2 $(d+1)$–*ribbon*

We shall now define the ribbon subclass of string d–links, which is characterized by the immersed balls that they can bound. Prior to its definition, we need hence to describe the singularities we shall allow for these immersed balls. We say that a connected singularity $\delta := Y_1 \cap Y_2 \subset \overset{*}{B}{}^{d+2}$ is *ribbon* if it is a transverse d–ball with two preimages:

- $\delta_c \subset \mathring{\tilde{Y}}_1$, that we shall call the *contractible preimage*;
- $\delta_{ess} \subset \tilde{Y}_2$, that we shall call the *essential preimage*, and for which it is required that $\mathring{\delta}_{ess} \subset \mathring{\tilde{Y}}_2$ and that $\partial\delta_{ess} \subset \partial_*\tilde{Y}_2$ represents a non trivial homology class in $\partial_*\tilde{Y}_2$.

In other words, a singularity is ribbon if it has two preimages, one which is lying in the interior of the immersed manifold—the contractible one, and the other which is properly embedded with boundary being homologically non trivial in the boundary of the immersed manifold—the essential one; see the right hand side of Figure I.5 for an illustration. This generalizes the notion of 3–dimensional ribbon singularities created by a ribbon passing through another one.

Definition 3.5. We define a $(d+1)$–*ribbon* as an immersion $\underset{i\in\{1,\dots,n\}}{\cup}(B^d \times I)_i$ of n copies of the $(d+1)$–dimensional ball in $B^{d+2} \cong B^{d+1} \times I$ such that, for every $i \in \{1,\dots,n\}$ and $\varepsilon \in \{0,1\}$, $\partial_\varepsilon(B^d \times I)_i = D^d_i \times \{\varepsilon\}$, and the singular set is a finite number of ribbon singularities.

To provide an orientation for a $(d+1)$–ribbon, it is sufficient to specify an orientation on its boundary and, by convention, we shall choose the one induced by D^d_i on $\partial_0(B^d \times I)_i$. Besides this $(d+1)$–dimensional orientation, a $(d+1)$–ribbon can be given a *co-orientation,* which is a 1–dimensional orientation for its *cores* $\underset{i\in\{1,\dots,n\}}{\cup}\big(\{0\}\times I\big)_i \subset \underset{i\in\{1,\dots,n\}}{\cup}(B^d \times I)_i$. Again by convention, we choose to orient the cores as going from $\partial_0 B^{d+2}$ to $\partial_1 B^{d+2}$.

3.1.3 *Ribbon string d–links*

Definition 3.6. A string d–link L is *ribbon* if $L = \partial_* R$ for some $(d+1)$–ribbon R. We say then that R is a *ribbon filling* for L. We denote by d–$r\mathrm{SL}_n$ the submonoid of ribbon string d–links.

We want to stress here the fact that ribbon string d–links are required to be fillable by a $(d+1)$–ribbon, but that the filling is not given. This will actually be the main issue to deal combinatorially with them. As a matter of fact, ribbon string d–links can be alternatively defined as the quotient of $(d+1)$–ribbons under isotopy and the equivalence relation generated by $R_1 \overset{\partial}{\sim} R_2 \Leftrightarrow \partial_* R_1 = \partial_* R_2$. Accordingly, we shall say that two $(d+1)$–ribbons differ by a *ribbon filling change* if their boundaries coincide.

3.2 Tube map

First defined for classical knots by T. Yajima in [Yaj62], and then extended to the welded case by S. Satoh in [Sat00], the Tube map is generally presented as an inflating process for welded diagrams. In this dissertation, we shall adopt an alternative, and somehow reversed, point of view, more intrinsically based on welded systems. It is an higher dimensions generalization of the approach given in [9].

3.2.1 *For* $(d+1)$–*ribbons*

We first define a map

$$\mathrm{Conn}\colon \big\{(d+1)\text{–ribbon}\big\}\big/_{\text{isotopy}} \longrightarrow \big\{\text{welded system}\big\}\big/_{\text{equivalence}}$$

which encodes the connexions between the ribbon singularities of a $(d+1)$–ribbon R as follows. Consider $\Delta := \{\delta_1,\dots,\delta_k\}$ the set of all its ribbon singularities or, equivalently, the set of their essential preimages. Each element of Δ is met by the core of the connected component of $\tilde{R}$ it belongs to, and this provides a, so-called, *co-orientation partial order* on Δ specified by $\delta_{i_1} \leq \delta_{i_2}$ iff δ_{i_1} and δ_{i_2} belong to the same component

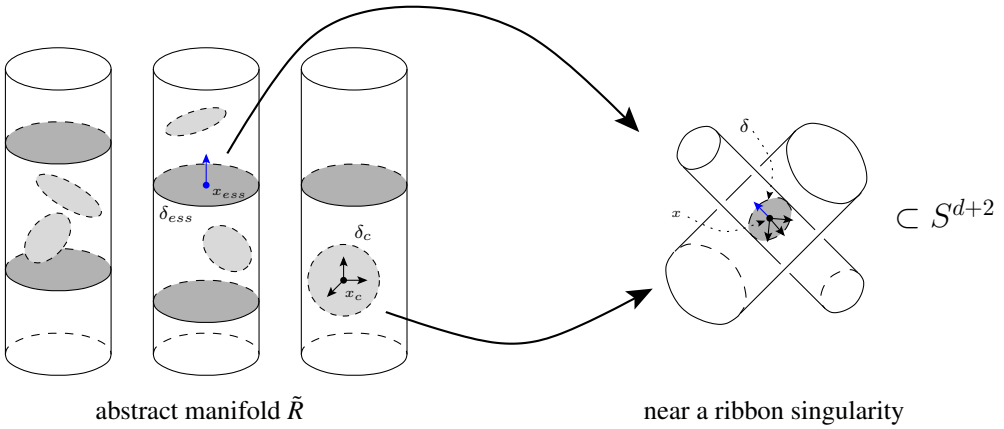


Figure I.5: Ribbon singularity and preimages

$(B^d \times I)_i$ of $\tilde{R}$, and the first intersection of the core of $(B^d \times I)_i$ with δ_{i_1} occurs before its first intersection with δ_{i_2}, according to the co-orientation of R. This partial order can be extended to $\Delta \sqcup \{1, \dots, n\}$ by identifying $i \in \{1, \dots, n\}$ with the preimage of $D_i^d \times \{0\} \subset \partial_0 R$.

Besides, the elements of Δ cut $\tilde{R}$ into a union of $(d+1)$–balls which can be seen as chambers glued along $\delta_1, \dots, \delta_k$; for each of these chambers, the boundary contains two d–balls either from Δ or from $\left\{D_i^d \times \{\varepsilon\} \mid i \in \{1, \dots, n\}, \varepsilon \in \{0, 1\}\right\}$. Ignoring the $D_i^d \times \{1\}$'s, this provides a one-to-one correspondence between the chambers and $\Delta \sqcup \{1, \dots, n\}$ which associates a chamber to the least element of $\Delta \sqcup \{1, \dots, n\}$ on its boundary according to the co-orientation partial order.

For each ribbon singularity δ, we moreover define a sign as follows. We first choose a point $x \in \mathring{\delta}$ and consider its preimages $x_c \in \delta_c$ and $x_{ess} \in \delta_{ess}$. Then we consider $(u_1, \dots, u_{d+1})$, the pushforward in $T_x B^{d+2}$ of a positive basis of $T_{x_c}\tilde{R}$, and v, the pushforward of a normal vector for $T_{x_{ess}}\delta_{ess} \subset T_{x_{ess}}\tilde{R}$ which points to the chamber associated to δ_{ess}. We say that δ is *positive* if $(u_1, \dots, u_{d+1}, v)$ is a positive basis for $T_x B^{d+2}$, and *negative* otherwise. See Figure I.5 for an illustration.

Finally, we note that the contractible preimages of the ribbon singularities are all disjoint from the essential ones; each of them is hence contained in one of the chambers.

Now, we can define $\mathrm{Conn}(R)$ as the poset $\Delta \sqcup \{1, \dots, n\}$, given with $t_{\mathrm{Conn}(R)} \colon \Delta \longrightarrow \Delta \sqcup \{1, \dots, n\}$ and $\sigma_{\mathrm{Conn}(R)} \colon \Delta \longrightarrow \{\pm 1\}$ where, for every $i \in \{1, \dots, k\}$

- $t_{\mathrm{Conn}(R)}(\delta_i)$ corresponds to the chamber to which the contractible preimage associated to δ_i belongs;
- $\sigma_{\mathrm{Conn}(R)}(\delta_i) = 1$ iff δ_i is positive.

Proposition 3.7. *The* Conn *map is a monoid isomorphism.*

Proof. Injectivity is by far the most intricate point. We shall sketch here the outlines of its proof.

Consider two $(d+1)$–ribbons R_1 and R_2 such that $\mathrm{Conn}(R_1) = \mathrm{Conn}(R_2)$. We first perform reparametrizations for R_1 and R_2 such that

1. each contractible preimage of a ribbon singularity δ belongs to the interior of a slice $\left(B^d \times \{t_\delta\}\right)_{i_\delta}$ of $\tilde{R}_1$ or $\tilde{R}_2$ for some $i_\delta \in \{1, \dots, n\}$ and $t_\delta \in I$;
2. for every ribbon singularity δ of R_1, $\left(i_{\xi(\delta)}, t_{\xi(\delta)}\right) = \left(i_\delta, t_\delta\right)$ where ξ is the one-to-one correspondence, induced by the equality $\mathrm{Conn}(R_1) = \mathrm{Conn}(R_2)$, between the ribbon singularities of R_1 and those of R_2.

The first point can be achieved by local deformation since preimages are contractible d–balls, and the second because the relative positions between preimages are the same in R_1 and R_2 since $\mathrm{Conn}(R_1) = \mathrm{Conn}(R_2)$.

Then, for every $\left(B^d \times \{t_\delta\}\right)_{i_\delta}$ with δ a ribbon singularity of R_1, we fix a small tubular neigborhood $U_\delta \subset \mathring{B}^{d+2}$ of its image; these are $(d+2)$–balls whose boundaries are met in, exactly, four d–balls by R_1—see the right hand side of Figure I.5. At that time, we perform an isotopy on R_2 such that, for every ribbon

singularity δ of R_1, $R_1 \cap U_\delta = R_2 \cap U_\delta$ as oriented and co-oriented spaces, the ribbon singularity of R_2 which superimpose with δ being $\xi(\delta)$. Again, this can be done since R_1 and R_2 are locally contractible.

Outside the U_δ's, R_1 and R_2 can now be seen as regular $(d+1)$–balls connecting the ends that come by four on each ∂U_δ together with the $D_i^{d+1} \times \{0\}$'s and the $D_i^{d+1} \times \{1\}$'s. Due to $\mathrm{Conn}(R_1) = \mathrm{Conn}(R_2)$ and condition 2, these connexions are combinatorially the same for R_1 and R_2; to conclude, it is hence sufficient to show that, up to isotopy, there is a unique way to embed $(d+1)$–balls in Y, where Y is B^{d+2} with a neighborhood of a finite number of points removed, such that they connect by pairs some given d–balls on ∂Y in a prescribed way. Note that, as a by-product, this would also show that Conn is surjective.

To prove this uniqueness property, one can notice that, up to isotopy, the $(d+1)$–balls are given by some 1–dimensional framed cores. Indeed, let B be such a $(d+1)$–ball that connect two boundary d–balls $B_0, B_1 \subset \partial Y$. Since B is regularly embedded, it can retract to a path which connect B_0 to B_1; and for each point x on this path, the positive normal vector to $T_xB \subset T_xB^{d+2}$ provides a normal framing. Reciprocally, any normally framed path γ from B_0 to B_1 can be inflated into a $(d+1)$–ball connecting B_0 to B_1 by considering, for every x on the path, a d–dimensional neigborhood of x which is orthogonal to both the derivative and the framing of γ. Now, since it has to stay orthogonal to the derivative of the path, the framing can be seen as a path on S^d, and it can actually be any path; but $d \geq 2$, so $\pi_1(S^d) = 1$ and all the framing are hence equivalent up to isotopy. The $(d+1)$–balls are thus given by just their 1–dimensional cores in Y, but since Y is a punctured $(d+2)$–ball with $d+2 \geq 4$, $\pi_1(Y) = 1$ and all cores are equivalent up to isotopy. □

Definition 3.8. We set

$$\widetilde{\mathrm{Tube}}\colon \left\{\text{welded system}\right\}\!/_{\text{equivalence}} \longrightarrow \left\{(d+1)\text{–ribbon}\right\}\!/_{\text{isotopy}}$$

as the inverse function of Conn.

3.2.2 For ribbon string d–links

Welded string links are the quotient of welded systems under R1, R2 and R3 moves. Ribbon string d–links can be seen as the quotient of $(d+1)$–ribbons under ribbon filling changes. But in [9], Figures 14–17 give explicitly some local ribbon filling changes which realize moves R1, R2 and R3 for welded systems. The pictures are given for $d = 2$, but they can be straightforwardly generalized to higher dimensions, using a map that inflates, in the $(d-2)$ missing dimensions, any point to a $(d-2)$–ball whose radius is a smooth function on the abstract manifold which is 1 on the contractible preimages of ribbon singularities and strictly greater than 1 anywhere else. Consequently, we obtain:

Proposition 3.9. *The* $\widetilde{\mathrm{Tube}}$ *map decends into a well defined surjective map* $Tube\colon wSL_n \longrightarrow d\text{–}rSL_n$.

The question whether the Tube map is injective or not remains open. We will return to this issue in the Perspectives section, but looking at our present task, we won't need to know its injectivity status to provide a classification up to link-homotopy.

3.3 Fundamental group

As usual, the *fundamental group* $\pi_1(L)$ of a, possibly self-singular, string d–link L is defined as $\pi_1(X_L)$, where X_L is the complement in B^{d+2} of a tubular neighborhood for L. This definition is general, but we shall now focus on the ribbon case. Except in the last paragraph, we shall hence assume now, within this section, that L is non singular and given with a ribbon filling R. Then we also denote by X_R the complement of R.

It is easily computed that $\pi_1(X_R)$ is trivial, and consequently, for every regular $x \in \mathring{R}$, we can unambiguously defined the *meridian* μ_x as the image in $\pi_1(L)$ of a loop in X_L which meets R exactly once, positively, in x. These meridians actually generates $\pi_1(L)$ since, generically, a loop in X_L meet R a finite number of times, and each of these intersections can be realized by some meridian or its inverse. As noticed in the previous section, R is cut into chambers by its ribbon singularities and, obviously, $\mu_x = \mu_y$ whenever x and y belongs to the same chamber. It is hence sufficient to consider one meridian for each chamber. In particular, for every $i \in \{1, \ldots, n\}$, we define the i^{th} *bottom* and *top meridians* as the meridians associated to the chambers which contain, respectively, $D_i^d \times \{0\}$ and $D_i^d \times \{1\}$ in their boundary.

These meridians satisfy some relations. Indeed, given a parametrized neighborhood of a ribbon singularity, a direct computation shows the following:

Lemma 3.10. *For every ribbon singularity δ of R, $\mu_{c_+} = \mu_{c_-}^{\mu_{c_0}^{\varepsilon}}$, where*

- *c_+ and c_- are the two chambers which contains δ in their boundary, c_+ being the direct successor of c_- according to the co-orientation partial order;*
- *c_0 is the chamber to which the contractible preimage of δ belongs;*
- *ε is the sign associated to δ.*

Actually, Lemma 3.10 provides a complete presentation for $\pi_1(L)$, but we won't need to know it. We shall rather focus on the fact that, as a consequence, every two meridians that belong to the same component of R are conjugate. It follows in particular that $\pi_1(L)$ is normally generated by either the bottom or by the top meridians and we can hence consider $\mathrm{R}\pi_1(L)$, the reduced quotient of $\pi_1(L)$ with regard to any of these two sets of generators.

Finally—and for any string 2–link, not only ribbon ones—we define, for every $i \in \{1, \dots, n\}$, a *i^{th} longitude for L* as any push out in X_L of a path on the i^{th} component of L, closed by a standard path on ∂B^{d+2}. The choice of path on the i^{th} component is actually irrelevant since, up to isotopy, any two choices differ by a loop in $C_i^{d-1} \times \{0\}$, but this loop can then be pushed out in $D_i^d \times \{0\}$ which is simply connected. On the contrary, the way the path is pushed out does matter and different choices may lead to longitudes which differ by a power of the i^{th} bottom meridian. Although it won't be crucial for our purpose, we should note that, as soon as a ribbon filling is given, say R, there is, for every $i \in \{1, \dots, n\}$, a preferred i^{th} longitude obtained by pushing out the path inside R or, equivalently, pushing it out such that it never meets R.

3.4 Ribbon link-homotopy

3.4.1 Seen from topology

We define now a seemingly restricted notion of link-homotopy for ribbon object. The point will be to allow link-homotopy but only in a way that preserve, in some sense, ribbonness. To this end, we introduce a notion of *critical ribbon singularity*, which is a transverse connected singularity $\delta := Y_1 \cap Y_2 \subset \mathring{B}^{d+2}$, homeomorphic to a d–ball and admitting two preimages:

- $\delta_c \subset \partial \tilde{Y}_1$, that we shall call the *contractible preimage*;
- $\delta_{ess} \subset \tilde{Y}_2$, that we shall call the *essential preimage*, and for which it is required that $\mathring{\delta}_{ess} \subset \mathring{\tilde{Y}}_2$ and that $\partial\delta_{ess} \subset \partial_* \tilde{Y}_2$ represents a non trivial homology class in $\partial_* \tilde{Y}_2$.

The only difference between a ribbon and critical ribbon singularity is that, for the former, the contractible preimage is entirely in the interior of the immersed manifold, whereas for the latter, it is stuck on the boundary. This is precisely the critical situation one faces when pushing at once a ribbon singularity out.

We can now define *singular $(d+1)$–ribbons* just as regular ones, but with the extra freedom that ribbon singularities may be critical and the extra requirement that exactly one is. We moreover say that a singular $(d+1)$–ribbon is *self-singular* if the two preimages of the critical ribbon singularity are on the same connected component of the abstract manifold. Accordingly, *self-singular ribbon string d–links* are then defined as the lateral boundary of self-singular $(d+1)$–ribbon. Note that singular ribbon string d–links are not anymore embedded, but immersed, since the boundary of the critical ribbon singularity is a singular double points locus.

Definition 3.11. Two ribbon string d–links L_1 and L_2 are said *elementary ribbon link-homotopic* if there is a smooth path $\gamma\colon I \longrightarrow \left\{(d+1)\text{–ribbon}\right\} \sqcup \left\{\text{self-singular } (d+1)\text{–ribbon}\right\}$ such that $\partial_*\gamma(0) = L_1$, $\partial_*\gamma(1) = L_2$ and $\gamma(t)$ is singular only for $t = \frac{1}{2}$. They are said *ribbon link-homotopic* if there is a finite sequence of ribbon string d–links $L'_1, \dots, L'_s$ such that $L'_1 = L_1$, $L'_s = L_2$ and L'_i is elementary ribbon link-homotopic to L'_{i+1} for every $i \in \{1, \dots, s-1\}$. We denote by $d\text{–}r\mathrm{SL}_n^{lh}$ the monoid of ribbon string d–links up to ribbon link-homotopy.

In rough words, a ribbon link-homotopy is a link-homotopy where the connected components are allowed to cross themselves only in a rigid way which can be locally filled by some ribbon $(d+1)$–balls. In particular, near each critical time of a ribbon link-homotopy, there is a given ribbon filling, and hence a set of ribbon singularity. When running through the critical time, the number of ribbon singularities may increase or decrease by one, but it may also be constant or be increased only at the critical time. However, these last two situations are non generic and can be avoided. Indeed, if considering the manifold $\cup_{t\in I}\gamma(t) \subset B^{d+2}\times I$, they corresponds to situations where the critical ribbon singularity is a tangential locus for the two involved components, and this can be perturbated so that they are not tangential anymore. As a matter of fact, one may assume that a ribbon link-homotopy contains only critical times for which the number of singularity changes by one.

3.4.2 Seen from the Tube *map*

Given a filled ribbon string d–link, one can make, up to ribbon link-homotopy, appear or disappear any ribbon singularity which has both its preimages in the same connected component by pushing it through the lateral boundary. When composed with the Conn map, this realizes a SV move on the associated welded systems. Reciprocally, any SV move on a welded system can be realized through the Tube map as a ribbon link-homotopy. It follows that:

Lemma 3.12. *The* Tube *map descends into a well defined surjective map* $\mathrm{Tube}\colon wSL_n^{sv} \longrightarrow d\text{–}rSL_n^{lh}$.

Actually, ribbon link-homotopy could have been defined as the smallest quotient of $d\text{–}r\mathrm{SL}_n$ such that the Tube map descends to a well defined map on $w\mathrm{SL}_n^{sv}$. Stated like this, ribbon link-homotopy may look rather artificial; but the above topological definition provides a more natural motivation and, as we shall see in Section 4, it actually coincides, at least in the $d = 2$ case, with the usual notion of link-homotopy.

3.5 Higher dimensional Artin–like invariant

To define a classifying invariant for string d–links up to ribbon link-homotopy, we shall adopt the very same strategy than Habbeger and Lin, recalled in Section 1.3. Let L be a string d–link and define X_L as the complement of a tubular neighborhood of L in B^{d+2}. It has been shown, in Section 3.3, that $\pi_1(L)$ is normally generated by either the bottom or by the top meridians of L. Moreover, it is straightforwardly computed that $\pi_1(\partial_0 X_L) \cong \pi_1(\partial_1 X_L) \cong \mathrm{F}_n$ and that the inclusion maps $\iota_\varepsilon\colon \partial_\varepsilon X_L \longrightarrow X_L$, for $\varepsilon \in \{0,1\}$ induces isomorphisms at the H_1 and H_2–levels. Then by Stallings theorem, refined by Habegger–Lin arguments, we obtain:

Lemma 3.13. *The maps* $\iota_0, \iota_1 : RF_n \longrightarrow R\pi_1(L)$ *are both group isomorphisms.*

In particular, $\mathrm{R}\pi_1(X_L)$ is homeomorphic to RF_n, and one can define the map $\varphi_L := \iota_0^{-1}\circ\iota_1$, which expresses the top meridians of L in terms of the bottom ones. Said differently, it sends the i^{th} generator to its conjugate by any i^{th} longitude.

Proposition 3.14 ([8, Prop. 2.33])**.** *If* L_1 *and* L_2 *are two ribbon string d–links which are ribbon link-homotopic, then* $\varphi_{L_1} = \varphi_{L_2}$.

In [8], the proof is given only for the $d = 2$ case, but once a ribbon filling is choosen, as a reverse process of the inflating map mentioned in Section 3.2.2, the general picture retracts to this case.

Definition 3.15. We define the d–dimensional Artin–like invariant as the group homomorphism

$$\mathrm{Art}_d\colon \left\{ \begin{array}{ccc} d\text{–}r\mathrm{SL}_n^{lh} & \longrightarrow & \mathrm{Aut}_{\mathrm{C}}(\mathrm{RF}_n) \\ L & \longmapsto & \varphi_L \end{array} \right. .$$

This topology-grounded Art_d map is actually closely related to the combinatorial Art_w map. Indeed, let W be a welded system and let R be the ribbon filling for $\mathrm{Tube}(W)$ given by $\widetilde{\mathrm{Tube}}$. Recall that, as a set, $W = \mathrm{Conn}(R) = \Delta_R \sqcup \{1,\dots,n\}$, where Δ_R is the set of ribbon singularities of R. In what follows, we shall furthermore identify each $i \in \{1,\dots,n\}$ with $D_i^d \times \{0\}$ and count them among the ribbon singularities. Then

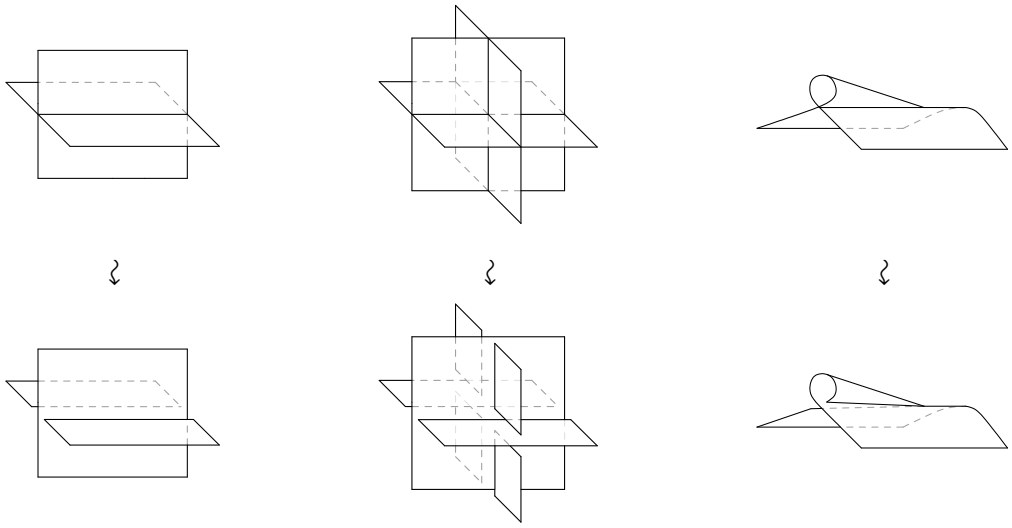


Figure I.6: Singularities in broken surface diagrams

we can define the map $\nu_R \colon W \longrightarrow \mathrm{RF}_n$ which send $a \in W = \mathrm{Conn}(R)$ to $\iota_0^{-1}(\mu_a)$, where μ_a is the reduced meridian associated to the chamber of R which contains a as the lowest ribbon singularity in its boundary, with respect to the co-orientation partial order. By Lemma 3.10, ν_R is actually a $(x_1, \dots, x_n)$–coloring for W; and by Proposition 2.10, it is the unique $(x_1, \dots, x_n)$–coloring of W. In particular, $\mathrm{Art}_w(W)$ is the map which sends x_i to the preimage by ι_0 of the i^{th} top meridian of $\mathrm{Tube}(W)$ or, in other words, to $(\iota_0^{-1} \circ \iota_1)(x_i)$. In other words:

Proposition 3.16. *$Art_w = Art_d \circ$ Tube.*

But, by Theorem 2.13, we know that Art_w is an isomorphism; up to ribbon link-homotopy, Tube is hence injective. But since it was already known to be surjective, it follows:

Proposition 3.17. *The map* Tube$\colon wSL_n^{sv} \longrightarrow d\text{–}rSL_n^{lh}$ *is a group isomorphism.*

And as a corollary, we obtain, whatever $d \geq 2$ is:

Theorem 3.18 ([6, Th. 5.1])**.** *The map $Art_d \colon d\text{–}rSL_n^{lh} \longrightarrow Aut_C(RF_n)$ is a group isomorphism.*

4 Classification of string 2–links up to link-homotopy

In this last section, we prove that, for $d = 2$, ribbon string 2–links and ribbon link-homotopy are both generic enough to provide a classification for general string 2–links up to usual link-homotopy. We shall start by developping a broken surface diagrams theory for immersed surfaces. In one hand, it will be used to prove that, as a corollary of Bartels–Teichner's theorem, every string 2–link is link-homotopic to a ribbon string 2–link; and on the other hand, that the Art_2 map is invariant under usual link-homotopy. The general classification will follow then from these two statements.

4.1 Broken surface diagrams

4.1.1 For embedded surfaces

Broken surface diagrams are the natural analogue of knot diagrams for embedded surfaces in dimension four, see *e.g.* [CS98, CKS04] for general overviews. They correspond to generic projections of the surfaces

onto B^3; this produces three kinds of singularities pictured in the upper row of Figure I.6: 1–dimensional loci of doubles points, and isolated triple and branch points. As illustrated in the lower row of Figure I.6, double points in broken surface diagrams are enhanced with an extra over/under information represented by erasing a small neighborhood in the sheet which is located below with regard to the projection direction. As for classical knots, a broken surface diagram with this over/under information is sufficient to recover, up to isotopy, the whole surface in B^4.

In [Ros98a], D. Roseman defined a finite set of local moves, now called *Roseman moves*; they are pictured up to reflections and mirror images[4] in Figure I.7. By *mirror image*, we mean the global swap of the over/under informations; it actually corresponds to a reflection in the projection direction. It can be noted that move (g) differs from the one given in [Ros98a], and that move (e) differs from the one given *e.g.* in [CKS04]; it is however easily seen that the three sets are equivalent and our choice has been determined by graphical and aesthetic consideration. D. Roseman proved the following:

Theorem 4.1 ([Ros98a])**.** *Two broken surface diagrams represent the same knotted surface iff they are connected by a finite sequence of Roseman moves.*

Broken surface diagrams provide hence a combinatorial way to see and study knotted surfaces.

4.1.2 For immersed surfaces

We want now to extend broken surface diagrams and Roseman moves to the singular setting. Unlike the 3–dimensional knot case, immersed surfaces in B^4 may have some isolated singular double points which cannot be removed by any small deformation. Generically, these singular points project on isolated points inside a 1–dimensional locus of double points, where the over/under information swaps. We denote these singular double points by a dot; see Figure I.8 for an illustration. We moreover say that a singular point is *self-singular* if both its preimages are on the same connected component.

Definition 4.2. A *(self-)singular broken surface diagram* is a generic projection into B^3 of an (self-)immersed surface in B^4, together with an over/under information for each line or circle of *regular* double points, that is double points which are not singular points. The *singular locus* of the broken surface diagram can refer either to the set of its double, triple, branch and singular points or to their preimages.

Of course, some additional moves on diagrams are required to generate isotopy and homotopy of immersed surfaces. These are the three *singular Roseman moves* given, up to reflections and mirror images, in Figure I.9. A singular Roseman move shall be said to be a *self-move* if it involves only self-singular points.

Following the same lines as in [Ros98a], we proved:

Proposition 4.3 ([6, Prop. 2.4])**.** *Two singular broken surface diagrams represent the same immersed surface in* 4*–space up to (link-)homotopy if and only if they are connected by a finite sequence of Roseman moves (a)–(g) and singular Roseman (self-)moves (h)–(j).*

As mentioned, the proof of Proposition 4.3 is essentially contained in Roseman's arguments for the embedded case and, actually, even the result is not surprising. It is indeed well-known, see *e.g.* [FQ90, Hir59], that regular (link-)homotopies are generated by ambient isotopies and finger/Whitney (self-)moves, and that general (link-)homotopies are furthermore generated by the additional cusp move. In our setting and up to the (a)–(g) Roseman moves, move (h) corresponds to isotopies, move (i) to finger/Whitney moves, and move (j) to cusp moves. As a matter of facts, Proposition 4.3 can be refined into

Proposition 4.4. *Two singular broken surface diagrams are connected by a finite sequence of Roseman moves (a)–(g) and*

- *singular Roseman moves (h) iff they represent the same immersed surface up to ambient isotopy;*
- *singular Roseman (self-)moves (h)–(i) iff they represent the same immersed surface up to regular (link-)homotopy;*

[4] this is actually not true: depending on the relative heights of the different sheets, move (e) has indeed a second version which is not equivalent to the pictured one, even up to reflections, and similarly, move (g) has five other versions; it is however easy to deduce them from the given pictures

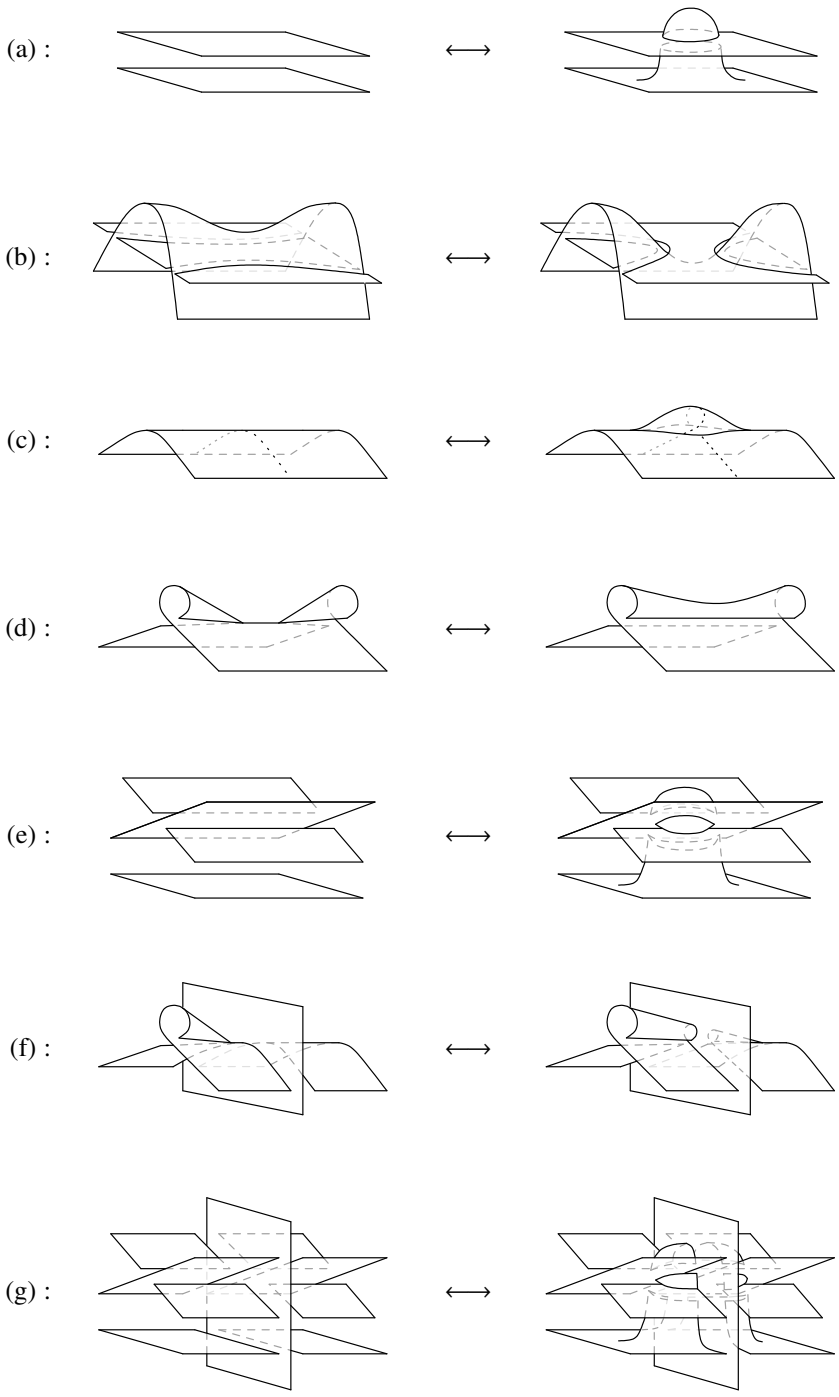


Figure I.7: Roseman moves:
for the move (c), a dotted path on the surface has been drawn to help visualizing the picture

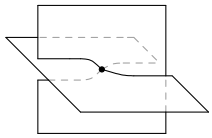


Figure I.8: Singular point in a broken surface diagram

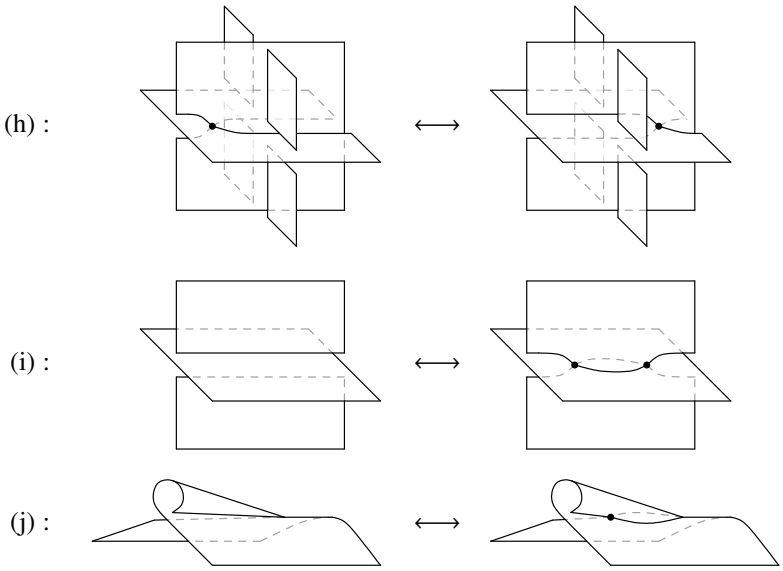


Figure I.9: Singular Roseman moves

- *singular Roseman (self-)moves (h)–(j) iff they represent the same immersed surface up to (link-)homotopy.*

Note however that Proposition 4.4 concerns the smooth category whereas [FQ90] deals with the topological one. Note also that in [Kam99], S. Kamada proved, in term of charts, a similar statement for *singular* 2*–braids* up to isotopy.

4.2 Ribbonness and link-homotopy

Regular and singular string 2–links have been defined as immersions of annuli $S^1 \times [0,1]$ in the 4–ball. The images of the circles $S^1 \times \left\{\frac{1}{3}\right\}$ and $S^1 \times \left\{\frac{2}{3}\right\}$ split each annulus into an *inner annulus*, namely $S^1 \times \left[\frac{1}{3}, \frac{2}{3}\right]$, and two *outer annuli*.

Definition 4.5. A *pseudo-ribbon diagram* for a, possibly singular, string 2–link is a broken surface diagram D such that the circles $S^1 \times \left\{\frac{1}{3}\right\}$ and $S^1 \times \left\{\frac{2}{3}\right\}$ are regular and their images bound embedded 2–discs, called *attaching discs*, satisfying:

- the interior of the attaching discs are disjoint from D;
- outer annuli are disjoint;
- each (connected component of the) intersection between an outer annulus A_{out} and an inner annulus A_{in} is a circle of regular double points whose preimages, in A_{out} is essential, and in A_{in} bounds a disk in A_{in} whose interior is disjoint from the singular locus of D.

Two pseudo-ribbon diagrams are called *equivalent* if they represent isotopic, possibly singular, string 2–links and *link-equivalent* if they represent link-homotopic, possibly self-singular, string 2–links.

Pseudo-ribbon diagram should be thought of as diagrams of knotted spheres—the inner annuli closed by the attaching discs, that we shall call the *inner spheres*—attached to the bottom and top boundaries by thin tubes—the outer annuli, that we shall also call *attaching tubes*—which are the lateral boundary of some 3–dimensional thickening of 1–dimensional strings, possibly linked with the spheres. It can be noted that the second condition implies that the attaching tubes without the inner spheres are embedded.

Pseudo-ribbon diagrams are rather flexible. First, every broken surface diagram for a string 2–link can be seen as pseudo-ribbon since, up to reparametrization, inner annuli can always be reduced to some collar neighborhoods of the bottom and top boundaries. Second, by pushing the attaching tubes out of the area first, every Roseman and singular Roseman moves can be performed on inner spheres; the following statement holds indeed true:

Lemma 4.6 ([6, Lem. 3.3 and proof of Th. 3.5])**.** *Let D be a pseudo-ribbon diagram and denote its inner spheres by S. If S' is a broken surface diagram for immersed spheres which is connected to S by a sequence of Roseman moves and singular Roseman (self-)moves, then there is a pseudo-ribbon diagram D', which is (link-)equivalent to D and whose inner spheres are S'.*

Yet, the "pseudo-ribbon" terminology is justified by the following:

Lemma 4.7 ([6, Lem. 3.4])**.** *A string 2–link admitting a pseudo-ribbon diagram with embedded*[5] *inner spheres is ribbon.*

Now, recall Bartels–Teichner theorem:

Theorem 4.8 ([BT99])**.** *Every smooth embedded spheres in B^4 are link-homotopically trivial.*

Then, for any string 2–link, we can choose a pseudo-ribbon diagram and perform on the inner spheres the link-homotopy prescribed by Bartels–Teichner theorem using Lemma 4.6. Applying then Lemma 4.7, we obtain that:

Theorem 4.9 ([6, Th. 3.5])**.** *Any string 2–link is link-homotopic to a ribbon one.*

Remark 4.10. Actually, Theorems 4.8 and 4.9 can be deduced each from the other. Indeed, reciprocally, every smooth embedded spheres can be cut open into a string 2–link L by removing small discs and stretching the result so that it is properly embedded. Then Theorem 4.9 asserts that L is link-homotopic to a ribbon string 2–links. Combining Proposition 3.17 and 2.4, we obtain that it is even link-homotopic to a monotonic ribbon string 2–link. But with the removed discs added back, such a monotonic ribbon string 2–link retracts to unknotted spheres.

4.3 Classification up to link-homotopy

The construction of the Art_2 map, defined in Section 3.5 for ribbon string 2–links, works actually for any string 2–links. The only point which need a further word is that the fundamental group is normally generated by either the bottom or by the top meridians, and this will be a consequence of the Wirtinger presentation given below. However, the construction fails for singular string 2–links since the embeddings of the bottom and top boundaries do not induce anymore epimorphisms at the H_2–level, and this prevents Stallings' theorem from being applied. But having Art_2 defined for self-singular string 2–link is nonetheless crucial if one wants to track it along a link-homotopy in order to prove its invariance. Indeed, contrary to the string link case, string 2–links along a link-homotopy are not singular only for a finite number of exceptional times. We shall hence provide an alternative definition for Art_2, more combinatorial and built on broken surfaces diagrams, which does extend to the self-singular setting.

4.3.1 Wirtinger presentation

A, possibly singular, broken surface diagram D for a, possibly singular, string 2–link L is an immersed oriented surface in B^3, with small bands removed to indicate the different projection heights of the sheets.

[5] in 3–space

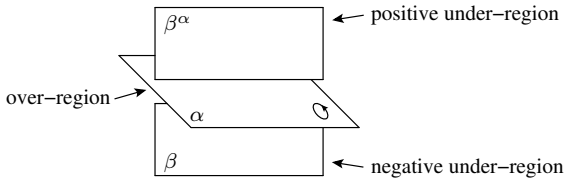


Figure I.10: Regions near a regular double point and RF_n–coloring

We define the *regions of D* as the connected components of D considered with these small bands and the singular points removed. Locally, there are hence three regions near a regular double point, seven near a triple point, two near a singular point and only one near a branch point; several of these local regions can however be the same if they are otherwise connected. Now, let p be a regular double point of D, and denote by S_o and S_u the sheets of D that meet at p such that S_o is over S_u with respect to the projection direction. We shall call *over-region of p* the region which belongs to S_o, and *under-regions of p* the other two. An under-region shall moreover be said *positive* or *negative*, depending on whether a basis of T_pB^3 made of a positive basis for T_pS_o concatenated with a vector of T_pS_u which points to the considered under-region, is positive or negative; see Figure I.10 for an illustration. For every $i \in \{1, \dots, n\}$, we finally call i^{th} *bottom* and *top regions* the unique regions that contain, respectively, $C_i \times \{0\}$ and $C_i \times \{1\}$.

To define $\pi_1(L)$, we fix a basepoint which is higher than any point of L in the projection direction. Then for each region r, we define $\mu_r \in \pi_1(L)$ as the loop which starts at the basepoint, runs straight above a given point $p \in r$, goes down along the projection direction, turns positively around p, that is along the boundary of a small oriented disc which meet positively L in p, and then goes back to the basepoint. In particular, for every $i \in \{1, \dots, n\}$, we define the *ith bottom* and *top meridians* as the meridians associated, respectively, to the i^{th} bottom and top regions.

Proposition 4.11 (*e.g.* [CKS04])**.**

- *For every regular double point p of D, $\mu_{r_+} = \mu_{r_-}^{\mu_{r_0}}$, where r_0 is the over-region, r_+ the positive under-region and r_- the negative under-region of p.*
- *For every singular point p of D, $[\mu_{r_1}; \mu_{r_2}] = 0$ where r_1 and r_2 are the two regions to which p is adherent.*

These relations provides actually a presentation for $\pi_1(L)$, called the *Wirtinger presentation*, which can be seen as a generalization of the presentation given in Section 3.3. Indeed, given a string 2–link L with a ribbon filling R, one can push R onto a neighborhood of $\{0\} \times B^2 \times I$ such that

- the ribbon singularities of R are all in $\{0\} \times B^2 \times I$;
- R is all in $\{0\} \times B^2 \times I$, except in a neighborhood of each essential preimage of its ribbon singularities, parametrized as $\big\{(x,t) \mid x \in B^2, t \in (-1,1)\big\}$, $B^2 \times \{0\}$ being the ribbon singularity, where the first coordinate in $B^3 \times I \cong B^1 \times B^2 \times I$ goes as $\varepsilon t e^{\frac{1}{t^2-1}}$, for some $\varepsilon \neq 0$, when t runs from -1 to 1.

When projecting along the first coordinate, we obtain a broken surface diagram D which, near ribbon singularity, looks locally like Figure I.11, and whose singular set is exactly the union of all the circles of regular double points which arise by pair near the ribbon singularities. It is immediately observed that regions of D, except for the small disk components each of whose boundaries comes from a circle of regular double points[6], are in one-to-one correspondence with chambers of R, as defined in Section 3.2.1, and it can be easily checked that the above relations and the relations given in Section 3.3 on the associated meridians are the same. In particular, the definitions of bottom and top meridians given above and in Section 3.3 do coincide.

Corollary 4.12. *For any, possibly singular, string 2–link L, $\pi_1(L)$ is normally generated by either the bottom or by the top meridians.*

[6] see for instance the small disk inside the thin tube in Figure I.11

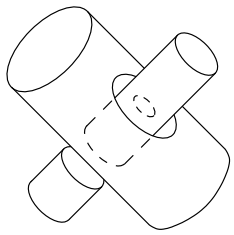


Figure I.11: Projecting a ribbon singularity in B^3

Consequently, the construction of the Art_2 map, given in Section 3.5 for ribbon string 2–links, can be extended to all (non-singular) string 2–links. Moreover, as a by-product of the construction, we also obtain that for any string 2–link L, $\mathrm{R}\pi_1(L)$ is isomorphic to RF_n generated by the bottom meridians, and that $\mathrm{Art}_2(L)$ sends x_i to the i^{th} top meridian, that is to its conjugate by a i^{th} longitude, defined in Section 3.3.

4.3.2 RF_n–colorings

To extend Art_2 to (at least some) self-singular string 2–links, we shall adopt a strategy which is close to what has been done for welded string links in Section 2.2.1.

Definition 4.13. An *RF_n–coloring* of a, possibly self-singular, broken surface diagram D for a, possibly self-singular, string 2–link is a map $\nu\colon \{\text{regions of } D\} \longrightarrow \mathrm{RF}_n$ such that:

- for every $i \in \{1, \dots, n\}$, the i^{th} bottom region is sent to the i^{th} generator of RF_n;
- for every regular double point p of D, $\nu(r_+) = \nu(r_-)^{\nu(r_0)}$ where r_0 is the over-region, r_+ the positive under-region and r_- the negative under-region of p.

No further condition is assigned to triple, branch nor singular points.

For any string 2–link L, a fundamental example of RF_n–coloring is the *Wirtinger coloring*, which sends each region to its associated meridian in $\mathrm{R}\pi_1(L) \cong \mathrm{RF}_n$. The map $\mathrm{Art}_2(L)$ can be deduced from it, since $\mathrm{Art}_2(L)$ sends the i^{th} generator to the image of the i^{th} top region under the Wirtinger coloring.

An RF_n–coloring is merely an example of surface diagram coloring, as considered *e.g.* in [CKS04]. As explained there or in [Ros98b], RF_n–colorings are somehow preserved by Roseman moves (a)–(g), in the sense that there is a one-to-one correspondence between the set of coloring before and after the move. It can indeed be checked, move by move, that knowing the values of the coloring on the regions which meet the boundary of the 3–ball supporting the move is sufficient to recover in a unique and consistent way the whole coloring inside the 3–ball. This is also clear for singular Roseman self-moves. This proves the following:

Lemma 4.14 ([6, Lem. 4.4])**.** *The number of possible RF_n–coloring for a, possibly singular, broken surface diagram of a, possibly singular, string 2–link is invariant under Roseman and singular Roseman moves.*

In the ribbon case, RF_n–colorings are closely related to the $(x_1, \dots, x_n)$–colorings defined in Section 2.2.1. Indeed, for a ribbon string 2–link L, one can fix a ribbon filling R and the associated—in the sense of the previous section—broken surface diagram D to see, using the correspondence between regions and chambers mentioned in the previous section and the correspondence between chambers and elements of the associated welded system mentioned in Section 3.2.1, that RF_n–colorings of D are in one-to-one correspondence with $(x_1, \dots, x_n)$–colorings of $\mathrm{Conn}(R)$. As a corollary of Theorem 4.9 and Proposition 2.10, we obtain hence:

Proposition 4.15 ([6, Prop. 4.5])**.** *For any broken surface diagram of either a string 2–link or a self-singular string 2–link which is link-homotopic to a string link, there is a unique RF_n–coloring. For broken surface diagrams of string 2–links, this is the Wirtinger coloring.*

Now if D_1 and D_2 are two broken surfaces diagrams for two, possibly singular, string 2–links which are link-homotopic, then they are connected by a finite sequence of Roseman moves and singular Roseman self-moves. If one fix a RF_n–coloring for D_1, then it will propagate all along the sequence, and at each step, the coloring will change only in the 3–ball which contains the move. As a result, the images of the top regions will remains the same for D_1 and D_2. If L is a string 2–link or a self-singular string 2–link which is link-homotopic to a string 2–link then, after Proposition 4.15, we can hence define a map $\mathrm{Art}_2(L) \in \mathrm{Aut}_{\mathrm{C}}(\mathrm{RF}_n)$ as the map which sends, for every $i \in \{1, \dots, n\}$, the i^{th} generator of RF_n to the image of the i^{th} top region under the unique RF_n–coloring of any broken surface diagram for L. We obtain for free that, for string 2–links, it coincides with the topology–grounded Art_2 map defined above, and that it is invariant under link-homtopy. Consequently:

Corollary 4.16. *The Art_2 map for string 2–links is invariant under link-homotopy.*

4.3.3 Conclusion

The stage is now set, and combining Theorem 4.9, Theorem 3.18 and Corollary 4.16, we obtain:

Theorem 4.17 ([6, Prop. 4.7])**.** *The map $Art_2 \colon 2\text{–}SL_n^{lh} \longrightarrow Aut_C(RF_n)$ is a group isomorphism.*

In the light of Corollary 1.9, this can be rephrased as:

Corollary 4.18 ([6, Th. 4.8])**.** *Up to link-homotopy, string 2–links are classified by non repeating Milnor numbers.*

Another corollary is that, at least for $d = 2$, the notion of ribbon link-homotopy appears to be equivalent to the usual link-homotopy in the sense that two ribbon string 2–links are ribbon link-homotopic iff they are link-homotopic.

Remark 4.19. The Art_2 invariant can be defined—and seen to classify $2\text{–}\mathrm{SL}_n^{lh}$—from scratch using only RF_n–colorings, without mentionning at all Habegger–Lin topological contruction and, in particular, without using Stallings' theorem. But what Habegger–Lin approach does provide is that the "combinatorial" longitudes in RF_n extracted from Art_2 using Corollary 1.9 are indeed "topological" longitudes in the reduced fundamental group.

Perspectives

Theorem 4.17 can be seen as a full accomplishment of the combinatorial welded knot theory in topology. Along the road, it opens a number of questions that we partially review now.

Injectivity of the Tube map

From the beginning of its study, an important question regarding the relationship between welded and ribbon objects remains open:

Question 1. *Is the* Tube *map injective ?*

Actually, this question splits in several subquestions as it can be asked for several type of objects. In this dissertation, we have indeed focus on the string link case, but welded knot theory can be extended to any kind of knotted objects such as links or braids. The Tube map is similarly defined toward the appropriate class of ribbon knotted surfaces.

Proposition 3.17 provides a positive answer up to link-homotopy, but the question is unanswered up to isotopy. However, when restricted to welded braids, which are welded string links staying transverse to the foliation $\sqcup_{t\in I} I \times \{t\}$, T. Brendle and A. Hatcher proved in [BH13b] that it is injective. On the other hand, for welded links, the *global reversal move* on welded diagrams—which essentially reverse all the signs and the partial order on arrows, and which is somehow related to the torus eversion in dimension 4—is known to let the Tube map invariant; see [Win09] and [9, Prop. 2.7 & 3.5]. Still, it is not known whether the Tube map is injective on welded links quotiented by global reversal moves.

For ribbon string 2–links, the boundary rigidity prevent eversions to be performed and the injectivity problem remains intact. As emphasized by Proposition 3.7 and Section 3.2.2, the main issue to deal with the Tube map is the question of ribbon filling changes. Moves R1, R2 and R3 correspond indeed to some local ribbon filling changes and Question 1 can be rephrased as:

Question 1.1.

- *Do these local changes generate all ribbon filling changes on string 2–links ?*
- *Do these local moves and the global change induced by the eversion generate all ribbon filling changes on knotted tori ?*

A strongly related question is the embedding of classical knotted objects among welded ones. Indeed, when restricted to welded diagrams with no virtual crossing, it is known that the Tube map is injective. This is due to the fact that links and string links are classified by their peripheral systems, and that the Wirtinger presentations provide a way to identify the fundamental group, the meridians and the longitudes of a classical object with the ones of its image under Tube. From this point of view, the global reversal move just corresponds to inverting the longitudes. Again, Question 1 can be rephrased as:

Question 1.2.

- *Are welded string links classified by their peripheral systems ?*
- *Are welded links classified by their peripheral systems up to longitude reversing ?*

Classification of string d–links up to link-homotopy

In the light of Theorem 4.17, Theorem 3.18 naturally raises the following question:

Question 2. *Are string d–links classified by* Art_d *?*

It is indeed easily seen that the fundamental group of any string d–link is normally generated by bottom and top meridians, so that Art_d can be defined for every string d–links. Following the $d = 2$ case, Question 2 reduces to:

Question 2.1. *Is* Art_d *invariant under link-homotopy ?*

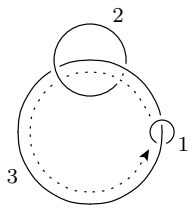


Figure I.12: A string 2–link which is no closure

Question 2.2. *Is any string d–link link-homotopic to a ribbon one ?*

Bartels–Teichner theorem, on which Theorem 4.9 strongly relies, holds in all dimension $d \geq 2$. It is hence very likely that the answer to Question 2.2 is yes. But to apply the same strategies than in Section 4, we are missing the d–dimensional counterpart of broken surface diagrams, that is a full control on the generic projection of string d–links on an hyperplane. Indeed, as we get higher in dimension, the singular locus of the projection get more intricate. This may be not an issue for generalizing RF_n–coloring and dealing accordingly with Question 2.1, since only regular double points are playing a role there; but it is for dealing with a higher dimensional analogue of Lemma 4.6.

A last question, which should be a corollary of Question 2 but may be answered on its own is the following:

Question 2.3. *Are ribbon and usual link-homotopies equivalent on ribbon string d–links ?*

Classification of torus-links up to link-homotopy

One of the main motivation of Habbegger and Lin classification of string links up to link-homotopy was the similar classification for links. Compared with Milnor seminal work in [Mil54], they indeed showed that the undeterminacy in Milnor invariants corresponds exactly to the undeterminacy when closing a string link into a link. Consequently, Milnor numbers are completely well defined for string links and, as stressed in Section 1.2, equivalent to the Art map when restricted to the non repeating ones. Besides, Habegger and Lin gave in [HL98] a classification scheme which provides an algebraic interpretation for the string links closure, and leads to a classification of links up to link-homotopy by a quotient of $\mathrm{Aut}_{\mathrm{C}}(\mathrm{RF}_n)$.

This classification scheme was succesfully applied in [8, Sec. 2.4] to ribbon torus-links—which are embedded tori in S^4 bounding some ribbon solid tori—up to link-homotopy. However, it does not apply to general torus-links—which are embedded tori in S^4—since they are not all the closure of a string 2–links. Indeed, in [6, Appendix A], we present an invariant of torus-links defined as the evaluation, for a given broken surface diagram, of the homology class in one torus-component of its intersection with another torus-component; computed on the broken surface diagram obtained by spinning the 3–component link shown in Figure I.12 around a line, and while spinning making the component 1 run a full turn around component 3, it shows that the underlying torus-link is not the closure of any string 2–link, even up to link-homotopy. This motivates the following:

Question 3. *Can torus–links be algebraically classified up to link-homotopy and how the ribbon subclass would fit inside this classification ?*

Classification of string 2–links up to concordance

Besides the relevance of welded knot theory for the study of knotted surfaces, Theorem 4.17 expresses also the substance of the ribbon subclass. One of the main point of the present dissertation is indeed that, up to link-homotopy, ribbon objects are simultaneously generic enough to provide an angle to the general case and rigid enough to be studied using tools inherited from the classical 3–dimensional knot theory.

One can wonder to what extent link-homotopy can be replaced by some weaker quotient while keeping their genericity to ribbon objects. In the light of general Milnor invariants, concordance is the second candidate after link-homotopy, and this leads to the following question:

Question 4. *Is any string* 2*–link concordant to a ribbon one ?*

A positive answer would immediately raise the following questions:

Question 5.

- *Can ribbon string* 2*–links be algebraically classified up to concordance ?*
- *Can string* 2*–links be algebraically classified up to concordance ?*

In the light of the classical concordance group complexity, and knowing that classical links embed in the ribbon subclass of knotted tori, Question 5 may look rather bold. Nevertheless, the concordance quotient for the image of classical objects under the Tube map may be simpler than the direct quotient for classical objects[7]. Moreover, the complexity of the classical concordance group is largely due to the failure of the Whitney trick in dimension 4; in higher dimension, the Whitney towers machinery should collapse, and with it the higher order Sato–Levine and Arf invariants [CST12], leaving Milnor invariants a possible set of classifying invariants.

A weaker form of Question 4 would be the following:

Question 6. *Is any string* 2*–link link-concordant to a ribbon one ?*

In view of the correspondance between Theorem 4.9 and Bartels–Teichner theorem, this statement may appear more reasonable as the latter builds on a theorem of Bartels which states that all embedded spheres are link-concordant to trivial ones. All the above questions can hence be recasted in terms of link-concordance.

Extensions of classical local moves

Although knot and link theory has its roots and foundations in the topology of embedded circles in 3–space, its study was early turned combinatorial by considering generic projections. This opened a new way to think the topology in terms of combinatorial local moves. First, ambient isotopies were proved in [Rei27] to correspond to Reidemeister moves (R1, R2, R3); then general homotopy to crossing changes (CC), link-homotopy to self-crossing changes (SC), link-homology—introduced by Murakami and Nakanishi [MN89] and Matveev [Mat87]–to delta moves (Δ). Other local moves were also investigated, still within some topological perspectives, such as the band-pass move (BP) which is motivated by the crossing of two bands, but also from more algebraic or even purely combinatorial considerations.

Welded knot theory is an extension of the classical knot theory and one can wonder what happen with the above interpretations of topological quotient in term of local moves. Since $\mathrm{Aut}^0_C(\mathrm{RF}_n) \subset \mathrm{Aut}_C(\mathrm{RF}_n)$, a by-product of Theorems 1.13 and 2.13 is that SV extends SC in the sense that two classical objects which are SV–equivalent in the welded realm are actually SC–equivalent in the classical one. Similar extensions for CC, BP and Δ to the welded case were investigated in [5]. Unexpectedly, it appeared that some moves can be extended in several distincts ways. For instance, CC can be extended by either itself or by the *virtualization move* (V)—which just remove any arrow in a welded system. The Δ move can also be extended by either the *fused move* (F)—which allow, for a welded system W, any permutation of the order on each W_i—or by the *virtual conjugation* (VC)—which exchange the role of the head and the tail in a arrow.

But welded knot theory can also be seen as some intermediate step toward ribbon knotted surfaces, and thus toward knotted surfaces. And besides, any classical local move induces a natural local move on broken surface diagrams by spinning it around a line. For instance, spinning SC leads to the *self-circle crossing change* (SCC), and it is easily seen that a ribbon link-homotopy can be realized using Roseman moves and SCC only. But on the other hand, SCC is a special case of link-homotopy and preserves hence the Art_2 map. It follows that if two ribbon string 2–links are SCC–equivalent, then they are SV–equivalent in the sense

[7] see, for instance, the complexity of the Kontsevitch integral [Kon93, Bar95] compared with the Alexander polynomial—which, up to the self–linking, is essentially the universal invariant for finite type invariants on welded knots [BD16]—although classical knots embed in welded ones

that they are the images under Tube of two SV–equivalent welded systems. In other words, SV can be seen as some residue of SCC, hence of SC, on the ribbon surfaces subclass. This residue point of view allows to distinguish a preferred extension between several. For instance, the spinning of CC—that is the circle crossing change (CCC)—is obviously an unknotting operation on ribbon string 2–links; but according to their classifying invariants given in [5, Sec. 3], V is an unknotting operation on welded systems while CC is not. It follows that, better than CC, V is the residue of CC on the ribbon subclass.

Question 7. *Is F the residue of* Δ *on the ribbon subclass ?*

As mentioned above, CC is a move which extends itself to the welded realm. This is not true for every move. One can indeed see that the classical trefoil can be unknotted using BP and welded moves, whereas the Arf invariant prevents this from happening within the classical theory. In [5], we introduced an *ad hoc* welded extension *w*BP of BP.

Question 8. *What is the residue of BP on the ribbon subclass, and how it is related to wBP ?*

Chapter II

From codes to quantum codes via (algebraic) topology

Introduction

In computer science, error-correcting codes were developed to detect and correct the errors that may occur while transmitting a message. The strategy is to embed the set of possible messages, seen as a $\mathbb{F}_2$–vector space, in a larger space so that the message can be coated with redundancy. All codes are not equally efficient, and the most common parameters to compare them are their *lengths*, corresponding to the length after coding, their *dimensions*, corresponding to the length before coding, and their *minimum distances*, which quantifies the maximal number of errors that can be corrected. Moreover, since decoding a general code is an NP–complete problem, the existence of some efficient[1] decoding algorithm for a given code is also of particular interest. In this respect, *LDPC* codes, introduced par R. Gallager in his PhD thesis [Gal62], have distinguished themeselves: families of such codes with increasing length have dimensions and minimum distances growing linearly with the length, and some low complexity *iterative decoding algorithms* can be applied on them with a capacity close to the Shannon limit [RSU01].

In quantum computer science, error-correction is all the more important as quantum decoherence eventually produces errors. Deemed impossible at first because of the no-cloning theorem, A. R. Calderbank, P. Shor [CS96] and, independently, A. Steane [Ste96] have nevertheless set up a, so-called, *stabilizator* coding scheme, enabling quantum error-correction. Among them, they more particularly brought to light the subclass of *CSS* codes. Although the classical and quantum theories of correcting codes are radically different, the notions of length, dimension and minimum distance are similarly found in the CSS code setting; and even LDPC code can be defined, which not only eases the conception of decoding algorithms—see for instance [PC08], but also the physical implementation since it reduces the set of qubits which are liable to interact. But more important, the data of a CSS code is equivalent to the data of two orthogonal classical codes, providing hence a natural angle for code theorists. From this point of view, the length and the dimension of the CSS code can be easily deduced from those of the two classical codes, but the minimum distance can only be bounded below. This approach has nevertheless been quite fruitful as, for instance, [Pos01], [MMM04], [COT07], [GFL08], [Hag08], [IM07], [Djo08], [SRK08], [Aly08], [AMT12], [TZ14], [CDZ13] or [Del12] can attest.

But combinatorially, the data of a CSS code corresponds also to a chain complex of length three given with a basis, and the correspondence can even be pushed further: the length of the code is equal to the dimension of the central space, the dimension is the dimension of the homology, and the minimum distance is the minimum weight for a representative of a non zero class in homology or in cohomology. This unexpected convergence of quantum codes and (algebraic) topology has been early observed by A. Kitaev, and it led to several fruitful applications; see [Kit03], [FM01], [FLM02], [BMD07], [Zém09] ou [10] for as many families of codes, all of which are LDPC.

[1] with polynomial complexity

Many LDPC families of CSS codes are hence known, based on disparate constructions. But one property gathers them all: contrary to the classical case, none of them has a minimum distance growing faster than the α^{th} power of the length, for any $\alpha > \frac{1}{2}$. In this regard, the best families are Freedman–Luo–Meyer's one, whose dimension grows as $\sqrt{n}$ and the minimum distance as $\sqrt{n\sqrt{\ln(n)}}$ where n is the length, and Tillich–Zémor's one, whose dimension is linear with the length and the minimum distance as the square root of the length. The question whether this square root barrier is fortuitous or not remains open, and a lot of effort is made to overcome it. It is with the idea that this barrier may be beaten by families of iterated powers that the work presented below has been initiated.

In the present dissertation, we deepen the interplay between chain complexes and CSS codes by transposing to the latter the standard notion of tensor product $\otimes$ defined for the former. Implicitely used in several previous constructions, we provide a formal framework for it. More precisely, we define two notions of product for CSS codes, a standard one $\otimes$, and a reduced one $\otimes_r$ with a slightly improved length. It should be mentioned that S. Bravyi et M. Hastings has already introduced an homological product $\boxtimes$ for a reduced class of CSS codes; although different, we shall see that the $\otimes$ and $\boxtimes$ products are closely related.

For $\otimes$ and $\otimes_r$, as well as for their iterated powers, we establish explicit formulas for the resulting parameters except the minimum distance which remains challenging to control. However—and this is actually the main result of the second part of this dissertation—we give a criterion of cohomological nature which provides a lower bound for the minimum distance of a product of CSS codes, the product being either $\otimes$, $\otimes_r$ or $\boxtimes$. It was somehow expected that, for two codes $\mathcal{C}$ and $\mathcal{D}$, the minimum distance of their product should be greater than both $d_{\mathcal{C}}$ and $d_{\mathcal{D}}$; but better than that, we obtain as a corollary of our criterion that, except in some trivial situations,

$$d_{\mathcal{C}\otimes\mathcal{D}}, d_{\mathcal{C}\otimes_r\mathcal{D}}, d_{\mathcal{C}\boxtimes\mathcal{D}} \geq 2\max(d_{\mathcal{C}}, d_{\mathcal{D}}).$$

This additional 2 factor has major consequences on the generic behavior of iterated powers. It follows indeed from it that the iterated powers of any honest CSS code generates an LDPC family with minimum distances tending exponentially to infinity. More surprising, even if a CSS code has no *quantum degeneracy*—which is, for a CSS code seen as two orthogonal classical codes $\mathcal{C}_1$ and $\mathcal{C}_2$, a minimum distance strictly greater than both the minimum distances of $\mathcal{C}_1$ and $\mathcal{C}_2$—its ℓ^{th} power, for ℓ large enough, does.

Using our criterion, we recover J-P. Tillich and G. Zémor's codes, given in [TZ14]. We also recover some Khovanov codes that we defined in [10]—and we take, by the way, this opportunity to recall their definition since they are also an occurence of a combinatorial model emerging from topology which is recycled in another field. We discuss the connections between $\otimes$ and $\boxtimes$ and explain how one can be extracted from the other. And finally, we provide three new families of CSS codes, respectively based on finite projective geometry, classical cyclic codes, and classical Reed–Muller codes. These three situations share the property of having a large group of automorphisms, and this facilitates the use of our criterion. Among all these families, the best one contains a subfamily which is almost LDPC—in the sense that the weight grows slower than any positive power of the length—with a dimension growing faster than the α^{th} power of the length and a minimum distance faster than the β^{th} power of the length, for any $\alpha < 1$ and any $\beta < \frac{1}{2}$, leaving open once again the square root barrier conjecture.

Notation and setting

We shall consider $\mathbb{F}$–spaces, which are finite-dimensional vector spaces over a field $\mathbb{F}$. All the theoretical material present in this paper can actually be adapted to work for any field but, in order to simplify notation, and since it is sufficient for all the applications we consider here, we restrict this presentation to the $\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$ case.

For any finite set $\Omega = \{x_1, \dots, x_s\}$, we shall denote by $|\Omega|$ its cardinality and by $\mathrm{Span}(x_1, \dots, x_s)$ the $\mathbb{F}_2$–space abstractly generated by its elements $x_1, \dots, x_s$. Now let C be any $\mathbb{F}_2$–space. We shall denote by $C^* := \mathrm{Hom}(C, \mathbb{F}_2)$ the dual space of C. Every map $f : A \to B$ induces a dual map $f^* : B^* \to A^*$ defined by $f^*(\varphi) = \varphi \circ f$ for every $\varphi \in B^*$. For every $X \subseteq C$, we denote its *orthogonal space* $\left\{\varphi \in C^* \mid \varphi_{|X} \equiv 0\right\}$ by $X^\perp$.

If C is given with a basis $\mathcal{B}$, then the bijection $\left(\mathcal{A} \subset \mathcal{B} \mapsto \sum_{b\in\mathcal{A}} b \in C\right)$ identifies the elements of C

with the subsets of $\mathcal{B}$. We shall freely use this identification, denoting subsets $\{a_1, \ldots, a_s\} \subset \mathcal{B}$, and hence the related elements of C, by unordered concatenations $a_1 a_2 \cdots a_s$. Associated to $\mathcal{B}$, there is a natural dual basis $\mathcal{B}^* := \left\{b^* \mid b \in \mathcal{B}\right\}$ for C^*, where b^* is defined by $b^*(b') = \delta_{bb'}$ for all $b' \in \mathcal{B}$. Here, δ stands for the Kronecker delta. Still using the subset identification mentioned above, we shall denote by $b \in x$, where $x \in C$ and $b \in \mathcal{B}$, the fact that $b^*(x) \neq 0$, which means that b appears in the decomposition of x; and by $|x|$ the Hamming weight of $x \in C$, which is the number of $b \in \mathcal{B}$ such that $b \in x$. We shall also denote with brackets the scalar product defined on C by $\langle b_1, b_2 \rangle := \delta_{b_1 b_2}$ for all $b_1, b_2 \in \mathcal{B}$. The following map:

$$\begin{array}{ccc} C & \longrightarrow & C^* \\ x & \longmapsto & y \mapsto \langle x, y \rangle \end{array}$$

is then an isomorphism sending $\mathcal{B}$ on $\mathcal{B}^*$. For every $X \subset C$, it induces an isomorphism between $X^\perp$ and $\left\{x \in E \mid \forall y \in C, \langle x, y \rangle = 0\right\}$. In order to reduce the amount of notation, we shall freely use this identification without mentionning it. The dual of a map $f : A \to B$ would hence be seen as $f^* : B \to A$, and it is easily checked that $\mathrm{Mat}_{\mathcal{B}^*}(f^*) = {}^t\mathrm{Mat}_{\mathcal{B}}(f)$.

By convention and unless otherwise specified, $\mathbb{F}_2$–spaces shall be denoted using roman capital letters, with an index i when it corresponds to the degree i part of a graded[2] space; chain complexes[1] using cursive capital letters; maps of chain complexes by ∂, possibly with a distinctive index or exponent; quantum codes[1] using calligraphic capital letters; and classical codes[1] using a slightly modified type of calligraphic capital letters. A same letter shall be used for associated objects: typically C shall be the CSS code[1] associated to the chain complex $\mathscr{C}$ defined as the 2–nilpotent[1] map ∂ (or $\partial_{\mathscr{C}}$) defined on $C := \bigoplus_{i \in \mathbb{Z}} C_i$. The map ∂_i shall be then the restricted map $\partial_{|C_i}$. If a classical code is involved in the story, then it should be $\mathcal{C}$.

1 CSS codes and chain complexes

1.1 Classical error-correcting codes

We begin by a very brief overview of classical error-correcting codes, but we refer the reader to [MS77] for a comprehensive survey. In classical computer engineering, information is modeled by sequences of *bits*, each of which is either 0 or 1. As a matter of fact, sequences of fixed length $n \in \mathbb{N}$ can be interpreted as vectors in $\mathbb{F}_2^n$, or more generally, as vectors in some n–dimensional $\mathbb{F}_2$–space given with a basis.

When transmitted, information can be altered, for instance by the swap of some of its bit values. Error-correcting codes are an attempt to overcomme this phenomenon by coating information with redundancy so that alterations of a small number of bits can be detected and possibly corrected. Accordingly, a *classical code* $\mathcal{C}$ is a subspace of an $\mathbb{F}_2$–space E given with a basis $\mathcal{B}_E$. For coding and decoding reasons, it is often more convenient to consider *linear codes* only, which are codes being actually vector subspaces. In this case, $\mathcal{C}$ can be described either by a generating map $g_{\mathcal{C}} : A \hookrightarrow E$ such that $\mathrm{Im}(g_{\mathcal{C}}) = \mathcal{C}$, or by a parity-check map $p_{\mathcal{C}} : E \twoheadrightarrow B$ such that $\mathrm{Ker}(p_{\mathcal{C}}) = \mathcal{C}$;and these maps can, in turn, be given by their matrices.

The efficiency of a given code $\mathcal{C} \subset E$ can be evaluated according to different parameters. The most common and obvious ones are:

- its *length* $n_{\mathcal{C}}$, defined as the dimension of E, which corresponds to the length of the message after coding;
- its *dimension* $k_{\mathcal{C}}$, defined as the dimension of $\mathcal{C}$, which corresponds to the length of the message before coding;
- its *minimum distance* $d_{\mathcal{C}}$, defined as the minimum weight for a non trivial element of $\mathcal{C}$, that is the minimum number of element of the basis $\mathcal{B}_E$ necessary to describe a vector in $\mathcal{C} \setminus \{0\}$, which corresponds to twice the number of errors that can be corrected.

There are, of course, many other parameters to analyse the strengths and the weaknesses of a classical code. The ability of being quickly decoded is, for example, particularly sought after. With this in mind, R. Gallager pointed out in his PhD thesis [Gal62] the remarkable efficiency of *low density parity-check (LDPC)* codes,

[2] see next sections for definitions

which are codes described by a sparse parity-check matrix: families of such codes with length tending to infinity have not only dimensions and minimum distances growing linearly with the length, but there also exist very efficient decoding algorithms for them [RSU01]. Consequently, we introduce a fourth parameter for $\mathcal{C}$, namely its *weight* $w_{\mathcal{C}}$, defined as the maximal weight of a row of $\mathrm{Mat}_{\mathcal{B}_E,\mathcal{B}_B}(p_{\mathcal{C}})$, where $p_{\mathcal{C}} : E \twoheadrightarrow B$ is a parity-check map for $\mathcal{C}$ and $\mathcal{B}_B$ is a given basis for B.

Finally, we define the *dual* of $\mathcal{C}$ as the code $\mathcal{C}^\perp \subset E^*$, which can alternatively be seen as $\left\{x \in E \;\middle|\; \forall y \in \mathcal{C}, \langle x, y\rangle = 0\right\} \subset E$. It is easily checked that $p^*_{\mathcal{C}}$ and $g^*_{\mathcal{C}}$ are, respectively, a generating map and a parity-check map for $\mathcal{C}^\perp$—so that, up to transpose, $\mathcal{C}$ and $\mathcal{C}^\perp$ exchange their generating and parity-check matrices—and that $n_{\mathcal{C}^\perp} = n_{\mathcal{C}}$ and $k_{\mathcal{C}^\perp} = n_{\mathcal{C}} - k_{\mathcal{C}}$.

1.2 From quantum errors to CSS codes

This section is a rough overview of error-corrrecting quantum codes adressed to non specialists. For more details, the interested reader is referred to [NC10], [Pre] or to the introduction of [Del12].

1.2.1 Qubits and their errors

In quantum theory, the elementary piece of information is the *qubit*. It is a unitary element in the $\mathbb{C}$–space $\mathcal{H}$ spanned by two generators, usually denoted by $|0\rangle$ and $|1\rangle$. We denote the space of qubits by $\mathcal{H}_1$. Actually, a qubit can be physically apprehended only up to $\mathbb{C}$–scalars, so that only its image in the projective quotient is relevant, but since it will be fruitful to deal with signs issues, we shall often switch between the (non commutative) affine and the (commutative) projective spaces. For convenience, we shall use notation with tildas each time we deal with affine elements.

Unlike the classical case, multiple qubits do not just concatenate: they can entangle. From the postulates of quantum mechanics, n qubits are described by unitary elements in $\mathcal{H}^{\otimes n}$; they are hence of the form $\sum_{x\in\{0,1\}^n} \alpha_x|x\rangle$ with $\sum_x |\alpha_x|^2 = 1$. We denote the space of such n–qubits by $\mathcal{H}_1^n$.

Transmitting, or even just keeping stored, an n–qubit may alter it. On a single qubit, a set of possible alterations is the Pauli group $\widetilde{\mathcal{G}}_1$, generated by three elements:

$$\widetilde{X}: \begin{array}{ccc} |0\rangle & \mapsto & |1\rangle \\ |1\rangle & \mapsto & |0\rangle \end{array}, \qquad \widetilde{Y}: \begin{array}{ccc} |0\rangle & \mapsto & -i|1\rangle \\ |1\rangle & \mapsto & i|0\rangle \end{array}, \qquad \widetilde{Z}: \begin{array}{ccc} |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & -|1\rangle \end{array}.$$

Of course, they are not the only errors which may occur, but they are an orthogonal basis for them. As we will see later, it is sufficient to focus our effort on them. We can note that every such Pauli error is of the form $\varepsilon\widetilde{A}$ with $\varepsilon \in S := \left\{\pm 1, \pm i\right\}$ and $\widetilde{A} \in \widetilde{E} := \left\{I, \widetilde{X}, \widetilde{Y}, \widetilde{Z}\right\}$ and that any two errors always do commute or anti-commute. We denote by $\mathcal{G}_1$ the projective quotient of $\widetilde{\mathcal{G}}_1$. It is an abelian group which is generated by only two elements, say X and Z, the images of $\widetilde{X}$ and $\widetilde{Z}$. On an n–qubit, every factor can be altered by an error. The group $\widetilde{\mathcal{G}}_n = \widetilde{\mathcal{G}}_1^{\otimes n}$, defined as the set $\widetilde{E}^n \times S$ with the obvious product, forms an orthogonal basis for errors on n–qubits. Here again, every two elements do commute or anti-commute; and the projective quotient $\mathcal{G}_n$ of $\widetilde{\mathcal{G}}_n$ is $\mathbb{E}^n$, where $\mathbb{E} := \left\{I, X, Z, XZ\right\}$. The group $\mathcal{G}_n$ is abelian but we say that two elements *commute* or *anti-commute* if, respectively, their lifts in $\widetilde{\mathcal{G}}_n$ do commute or anti-commute. Note that it does not depend on the choosen lifts.

For every $A \in \left\{X, Y, Z\right\}$, we say that an error $E \in \mathcal{G}_n$ is of *type* A if it belongs to $\mathbb{E}_A^n$, where $\mathbb{E}_A := \left\{I, A\right\}$, that is if it acts on every qubit by either I or A. It is straightforwardly checked that two errors of same type commutes whereas errors of different kinds anti-commute.

1.2.2 CSS codes

A *quantum code* C of length $n \in \mathbb{N}^*$ and dimension $k \in [\![1, n]\!]$ is a 2^k–dimensional subspace of $\mathcal{H}^{\otimes n}$; a *codeword* is any of its elements. It makes possible the storage of a k–qubit in the form of an n–qubit, what enables, as we shall see, a correction process for small alterations of the codewords. The terminology, here, may be misleading since the dimension of a quantum code refers to the number of encoded qubits and not to the actual dimension of the code as a $\mathbb{C}$–space.

Let G be a subgroup of $\mathcal{G}_n$ such that G is liftable to a group $\widetilde{G} \subset \widetilde{\mathcal{G}}_n$. For every $g \in G$, we denote by $\widetilde{g}$ its lift in $\widetilde{G}$. We define C_G as $\mathrm{Fix}_{\widetilde{G}}(\mathcal{H}_1^n) := \left\{x \in \mathcal{H}_1^n \mid \forall \widetilde{g} \in \widetilde{G}, \widetilde{g}(x) = x\right\}$; this actually depends only on G and not on the choosen lift $\widetilde{G}$.

Lemma 1.1. *If G is generated by $(n-k)$ independent elements of $\mathcal{G}_n$, then C_G is a quantum code, so-called* stabilizer code*, of dimension k.*

Definition 1.2. A *CSS* code is a stabilizer code C_G given with a set of generators for G which are all of type either X or Z.

Since $\mathbb{E}_X^n$ and $\mathbb{E}_Z^n$ are both abelian and made of order 2 elements, they are both isomorphic to $\mathbb{F}_2^n$. As a matter of fact, such a set of generators can be described as the rows of two matrices $\mathbf{H}_X, \mathbf{H}_Z \in \bigcup_{p \in \mathbb{N}^*} \mathrm{Mat}_{\mathbb{F}_2}(p,n)$: to a row $(a_1, \cdots, a_n) \in \mathbb{F}_2^n$ of $\mathbf{H}_A$ with $A = X$ or Z, we associate $(A^{a_1}, \cdots, A^{a_n}) \in \mathbb{E}_A^n$.

The fact that G is liftable in $\widetilde{\mathcal{G}}_n$ means that every two generators x and y commute. Of course, if $x, y \in \mathbb{E}_X^n$ or $x, y \in \mathbb{E}_Z^n$, this is trivially satisfied; but since $\widetilde{X}$ and $\widetilde{Z}$ anticommute, $x \in \mathbb{E}_X^n$ and $y \in \mathbb{E}_Z^n$ do commute iff they share an even number of non-zero entries, that is if the product of the associated rows in $\mathbf{H}_X$ and in $\mathbf{H}_Z$ is zero.

Finally, generators in $\mathbb{E}_X^n$ are necessarily independent from those in $\mathbb{E}_Z^n$, so the minimal number of independent generators for G is $\mathrm{rk}(\mathbf{H}_X) + \mathrm{rk}(\mathbf{H}_Z)$. As a matter of fact, two matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ such that $\mathbf{H}_X {}^t\mathbf{H}_Z = 0$ describe a CSS code C whose length n is equal to their common number of columns, and whose dimension is $k = n - \mathrm{rk}(\mathbf{H}_X) - \mathrm{rk}(\mathbf{H}_Z)$. We also define the *weight* of C has the maximal weight—which is the maximal number of non trivial entries—of a row in $\mathbf{H}_X$ or in $\mathbf{H}_Z$; however, this parameter is not intrinsically associated to C but to the matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ and depends hence on a choice of generators for G.

As a conclusion, we observe that since CSS codes are given by two matrices whose product is null, they can be interpreted as pairs of classical codes which are orthogonal, in the sense that each is contained in the orthogonal of the other. In Section 1.3.3, we will give another interpretation related to algebraic topology.

1.2.3 Decoding and minimum distance

In quantum physics, measurements can be seen as orthogonal projections. More precisely, for a given orthogonal decomposition $\mathcal{H}^n = \overset{\perp}{\oplus} V_i$, there is an associated measure which sends a unitary element $\sum x_i \in \mathcal{H}_1^n$ to $\frac{1}{\|x_{i_0}\|} x_{i_0}$ with probability $\|x_{i_0}\|^2$.

Now, let C_G be a CSS code and $\{E_1, \cdots, E_{n-k}\}$ be a minimal set of $n-k$ generators for G. For every $\sigma := (s_1, \cdots, s_{n-k}) \in \mathbb{F}_2^{n-k}$, we set $C(\sigma) := \{x \in \mathcal{H}_1^n \mid \forall i \in [\![1, n-k]\!], \widetilde{E}_i(x) = (-1)^{s_i} x\}$. For every error $E \in \mathcal{G}_n$, we define its syndrome $\sigma(E) := \left(s_1(E), \cdots, s_{n-k}(E)\right) \in \mathbb{F}_2^{n-k}$ by $s_i(E) = 0$ iff E commutes with E_i. We can note that if $x \in C_G$ and $E \in \mathcal{G}_n$, then $\widetilde{E}(x) \in C(\sigma(E))$. The *weight of an error* is the number of qubits it alters. For every $\sigma \in \mathbb{F}_2^{n-k}$, we choose a minimally weighted error E_σ of syndrome σ.

The decomposition $\mathcal{H}^n = \overset{\perp}{\bigoplus_{\sigma \in \mathbb{F}_2^{n-k}}} C(\sigma)$ holds and the associated measure μ discretizes the set of possible alterations of a codeword. Now, let $e(x_0)$ be a codeword $x_0 \in C_G = \mathrm{Fix}_{\widetilde{G}}(\mathcal{H}_1^n)$ altered by an error e and assume that μ projects it to $E(x_0)$ where E is a Pauli error of syndrome σ_E. Then one can try to correct the error by computing $\overline{x_0} := \widetilde{E}_{\sigma_E} \widetilde{E}(x_0)$. By construction, $\widetilde{E}_{\sigma_E} \widetilde{E}$ has a syndrome equal to zero, so it commutes with all elements in G. If it is actually in G, then $\overline{x_0} = x_0$ and we got back the initial codeword. However, it may happen that $\widetilde{E}_{\sigma_E} \widetilde{E}$ does not belong to G, and the decoding process then fails.

The *minimum distance* of a code is the minimal weight of a non detectible error that does alter codewords. For a CSS code C_G, it is the minimal weight of an error which commutes with all the elements of G but does not belong to G. It corresponds, as we will see in the proof of Proposition 1.15, to the minimal weight of a vector which is in the kernel of one of the matrices $\mathbf{H}_X$ or $\mathbf{H}_Z$ without being spanned by the rows of the other.

Like in the classical case, efficient decoding algorithm often come with matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ which are sparse in the sense that the weight is small compared to the length [PC08]. We say that a family $(C_\ell)_{\ell \in \mathbb{N}}$ is *LDPC* if the weight of C_ℓ increases at most as the logarithm of the length of C_ℓ when ℓ goes to infinity.

Notation 1.3. For any code, we denote its parameters by $[\![n, k, d, w]\!]$, or $[\![n, k, d]\!]$ if ommiting w, where n is the length of the code, k its dimension, d its minimum distance and w its weight.

1.3 From chain complexes to CSS codes

Here, we review some basic notions of algebraic topology and relate them to CSS codes. For further details, we refer the interested reader to [Wei94], [HS97], [ML95] or [Lan02].

1.3.1 Definitions

In the litterature, chain complexes are often defined as sequences of $\mathbb{F}$–spaces $(C_i)_{i\in\mathbb{Z}}$ which are all zero but a finite number of them, together with a collection of linear maps either all of the form $\partial_i : C_i \to C_{i+1}$ or all of the form $\partial_i : C_i \to C_{i-1}$. An alternative way to describe them is to consider the direct sum $C := \bigoplus_{i\in\mathbb{Z}} C_i$ and regard the collection of maps $(\partial_i)_{i\in\mathbb{Z}}$ as a graded endomorphism of C. In the present dissertation, we shall adopt the latter approach.

Definition 1.4. A linear map $\partial \in \mathrm{End}(C)$, for some $\mathbb{F}_2$–space C, is 2–nilpotent if it satisfies $\partial^2 = 0$.
An ε–chain complex $\mathscr{C}$, for $\varepsilon = \pm 1$, is a 2–nilpotent map $\partial \in \mathrm{End}(C)$ such that

- C is $\mathbb{Z}$–graded, that is it decomposes into $C := \bigoplus_{i\in\mathbb{Z}} C_i$;
- ∂ shifts the degree by exactly ε, that is $\mathrm{Im}(\partial_{|C_i}) \subset C_{i+\varepsilon}$ for every $i \in \mathbb{Z}$.

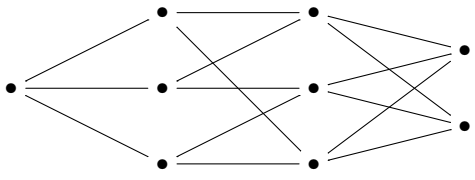
If omitted, ε shall be assumed to be $+1$.

Since C is finite-dimensional, there is only a finite number of degrees i such that $C_i \neq \{0\}$. The *support* of a non trivial chain complex $\mathscr{C}$ is the smallest interval $\{a, a+1, \ldots, b-1, b\}$ of integers such that $C_i = \{0\}$ for $i < a$ or $i > b$; we say that $\mathscr{C}$ is *k–length*, for $k \in \mathbb{N}^*$, if $b - a + 1 \leq k$. A *basis $\mathcal{B}$ for $\mathscr{C}$* is the data of a basis for each space C_i, that is an identification of C_i with a power of $\mathbb{F}_2$; we say then that $\mathscr{C}$ is *based.*

Notation 1.5. Chain complexes shall be represented as

$$\cdots \xrightarrow{\partial_{i-2}} C_{i-1} \xrightarrow{\partial_{i-1}} C_i \xrightarrow{\partial_i} C_{i+1} \xrightarrow{\partial_{i+1}} C_{i+2} \xrightarrow{\partial_{i+2}} \cdots .$$

In explicit based cases, C_i shall be represented by dots set vertically, one for each generator, and ∂_i shall be represented by edges joining a generator x to the elements of $\partial_i(x)$. For instance, the following picture:



represents the complex $\mathrm{Span}(x_1^1) \xrightarrow{\partial_1} \mathrm{Span}(x_1^2, x_2^2, x_3^2) \xrightarrow{\partial_2} \mathrm{Span}(x_1^3, x_2^3, x_3^3) \xrightarrow{\partial_3} \mathrm{Span}(x_1^4, x_2^4)$, where

- x_j^i is the generator represented by the j^{th} dot, from top to bottom, in the i^{th} column, from left to right;
- $\partial_1(x_1^1) = x_1^2 + x_2^2 + x_3^2$, $\partial_2(x_1^2, x_2^2, x_3^2) = (x_1^3 + x_3^3, x_1^3 + x_2^3, x_2^3 + x_3^3)$ and $\partial_3(x_1^3) = \partial_3(x_2^3) = \partial_3(x_3^3) = x_1^4 + x_2^4$.

This graph notation has the drawback to leave out the degrees which are then given only up to a global shift; this should however not be a problem for the purpose of the present dissertation.

Definition 1.6. For any ε–chain complex $\mathscr{C}$, we define its dual $\mathscr{C}^*$ as the $(-\varepsilon)$–chain complex $\partial^* \in \mathrm{End}(C^*)$ defined by $C^* := \bigoplus_{i\in\mathbb{Z}} \mathrm{Hom}(C_i, \mathbb{F})$ and $\partial^*(\varphi) = \varphi \circ \partial$ for every $\varphi \in C^*$.

If $\mathscr{C}$ is based, then the maps ∂_i can be given by their matrices. Using the identification between an $\mathbb{F}_2$–space and its dual mentioned in the Notation section, $\mathscr{C}^*$ can be seen as the chain complex obtained by reversing all the arrows and transposing all the matrices. In particular, if $\mathscr{C}$ is given by a graph as in Notation

1.5, then $\mathscr{C}^*$ is given by reading the graph from right to left. We say that a chain complex $\mathscr{C}$ is *symmetric* if it is presented by a graph G whose left/right mirror image is, up to reordering the dots in each column, again G. It implies, in particular, that $\mathscr{C}$ and $\mathscr{C}^*$ are isomorphic.

Definition 1.7. For any ε–chain complex $\mathscr{C}$, we define its *homology groups* $H_\bullet(\mathscr{C}) := \bigoplus_{i\in\mathbb{Z}} H_i(\mathscr{C})$ by $H_i(\mathscr{C}) := \mathrm{Ker}(\partial_i)/\mathrm{Im}(\partial_{i-\varepsilon})$. For any $x \in \mathrm{Ker}(\partial)$, we denote by $[x]$ its class in $H_\bullet(\mathscr{C})$. Homology groups of $\mathscr{C}^*$ are also called *cohomology groups* of $\mathscr{C}$ and denoted by $H^\bullet(\mathscr{C}) := \bigoplus_{i\in\mathbb{Z}} H^i(\mathscr{C})$. We say that $\mathscr{C}$ is *acyclic* if all its homology groups are trivial.

It can be noted that, for every $f \in C_i^*$, $f \in \mathrm{Ker}(\partial_{i-\varepsilon}^*)$ iff $f_{|\mathrm{Im}(\partial_{i-\varepsilon})} \equiv 0$, that is iff f induces a well defined map $\bar{f}$ on $H_i(\mathscr{C})$; and moreover that $f \in \mathrm{Im}(\partial_i)$ iff $f_{|\mathrm{Ker}(\partial_0)} \equiv 0$, that is iff $\bar{f} \equiv 0$. It follows:

Proposition 1.8. *For every chain complex $\mathscr{C}$ and every $i \in \mathbb{Z}$, $H^i(\mathscr{C}) \cong H_i(\mathscr{C})^*$.*

As we shall see later, chain complexes are closely related to CSS codes and the parameters of the latter reflect into parameters for the former, that we define now.

Definition 1.9. If $\mathscr{C}$ is a ε–chain complex given with a basis $\mathcal{B}$, then, for each $i \in \mathbb{Z}$ we denote by

- $n_i(\mathscr{C}) := \dim(C_i)$ and define the *length* of $\mathscr{C}$ as $n_\mathscr{C} := n_0(\mathscr{C})$;
- $k_i(\mathscr{C}) := \dim\big(H_i(\mathscr{C})\big)$ and define the *dimension* of $\mathscr{C}$ as $k_\mathscr{C} := k_0(\mathscr{C})$;
- $d_i(\mathscr{C}) := \min\big\{|x| \;\big|\; [x] \in H_i(\mathscr{C}) \setminus \{0\}\big\}$, with the convention that $\min\emptyset = \infty$, and define the *minimum distance* of $\mathscr{C}$ as $d_\mathscr{C} := d_0(\mathscr{C})$;
- $w_i(\mathscr{C}) := \max\big\{|x| \;\big|\; x \text{ row of } \mathrm{Mat}_\mathcal{B}(\partial_i)\big\}$ and define the *weight* of $\mathscr{C}$ as $w_\mathscr{C} := w_0(\mathscr{C})$.

Remark 1.10. The above parameters have only a relative dependency with regard to the basis. Indeed, $w_\mathscr{C}$ depends only on the restriction of $\mathcal{B}$ to $C_{-1} \sqcup C_0 \sqcup C_1$, $d_\mathscr{C}$ depends only on its restriction to C_0, $n_\mathscr{C}$ and $k_\mathscr{C}$ are independant of $\mathcal{B}$.

1.3.2 Operations on chain complexes

Chain complexes are naturally endowed with sum and product operations. We now recall them and, as far as possible, we make explicit how the parameters defined in the previous section behave with regard to these operations.

Definition 1.11. Let $\mathscr{C}$ and $\mathscr{D}$ be two ε–chain complexes. We define their direct sum $\mathscr{C} \oplus \mathscr{D}$ as the ε–chain complex $\partial_\mathscr{C} \oplus \partial_\mathscr{D} \in \mathrm{End}\Big(\bigoplus_{i\in\mathbb{Z}} \big(C_i \oplus D_i\big)\Big)$.

Proposition 1.12. *Let $\mathscr{C}$ and $\mathscr{D}$ be two ε–chain complexes. Then $\big(\mathscr{C} \oplus \mathscr{D}\big)^* \cong \mathscr{C}^* \oplus \mathscr{D}^*$ and for each $i \in \mathbb{Z}$,*

- *$H_i(\mathscr{C} \oplus \mathscr{D}) \cong H_i(\mathscr{C}) \oplus H_i(\mathscr{D})$;*
- *$n_i(\mathscr{C} \oplus \mathscr{D}) = n_i(\mathscr{C}) + n_i(\mathscr{D})$ and $k_i(\mathscr{C} \oplus \mathscr{D}) = k_i(\mathscr{C}) + k_i(\mathscr{D})$;*
- *if $\mathscr{C}$ and $\mathscr{D}$ were given with bases $\mathcal{B}_\mathscr{C}$ and $\mathcal{B}_\mathscr{D}$, then $\mathcal{B}_\mathscr{C} \sqcup \mathcal{B}_\mathscr{D}$ provides a basis for $\mathscr{C} \oplus \mathscr{D}$ such that $d_i(\mathscr{C} \oplus \mathscr{D}) = \min\big(d_i(\mathscr{C}), d_i(\mathscr{D})\big)$ and $w_i(\mathscr{C} \oplus \mathscr{D}) = \max\big(w_i(\mathscr{C}), w_i(\mathscr{D})\big)$.*

In particular, we emphasize the fact that adding an acyclic based direct summand does not affect the parameters except the length which is increased consequently. But conversely, detecting and removing an acyclic direct summand may alter the minimum distance if the basis does not respect the direct sum decomposition.

Definition 1.13. Let $\mathscr{C}$ and $\mathscr{D}$ be two ε–chain complexes. We define the tensor product $\mathscr{C} \otimes \mathscr{D}$ as the ε–chain complex $\mathrm{Id}_C \otimes \partial_\mathscr{D} + \partial_\mathscr{C} \otimes \mathrm{Id}_D \in \mathrm{End}\Big(\bigoplus_{i\in\mathbb{Z}} \big(\bigoplus_{r\in\mathbb{Z}} (C_r \otimes D_{i-r})\big)\Big)$.

Proposition 1.14. *Let $\mathscr{C}$ and $\mathscr{D}$ be two ε–chain complexes. Then $\big(\mathscr{C} \otimes \mathscr{D}\big)^* \cong \mathscr{C}^* \otimes \mathscr{D}^*$ and for each $i \in \mathbb{Z}$,*

- *$H_i(\mathscr{C} \otimes \mathscr{D}) \cong \bigoplus_{r\in\mathbb{Z}} \big(H_r(\mathscr{C}) \otimes H_{i-r}(\mathscr{D})\big)$ (Künneth formula);*

- $n_i(\mathscr{C}\otimes\mathscr{D}) = \sum_{r\in\mathbb{Z}} n_r(\mathscr{C}).n_{i-r}(\mathscr{D})$ *and* $k_i(\mathscr{C}\otimes\mathscr{D}) = \sum_{r\in\mathbb{Z}} k_r(\mathscr{C}).k_{i-r}(\mathscr{D})$*;*
- *if* $\mathscr{C}$ *and* $\mathscr{D}$ *were given with bases* $\mathcal{B}_{\mathscr{C}}$ *and* $\mathcal{B}_{\mathscr{D}}$*, then* $\mathcal{B}_{\mathscr{C}}\otimes\mathcal{B}_{\mathscr{D}}$ *provides a basis for* $\mathscr{C}\otimes\mathscr{D}$ *such that* $w_i(\mathscr{C}\otimes\mathscr{D}) = \max\left\{w_j(\mathscr{C}) + w_k(\mathscr{D}) \middle| j+k=i\right\}$.

Evaluating $d_i(\mathscr{C}\otimes\mathscr{D})$ is a much more involved problem and it will actually be the main concern of Section 2.

1.3.3 Chain complex and codes

In Section 1.2.2, CSS codes were roughly defined as pairs of matrices whose product is null. If these matrices are thought of as the matrices of some linear maps, then the product condition reduces to the composition of the maps being null. In other words, they describe a 3–length chain complex. Conversely, to any 3–length piece of based chain complex $\mathscr{C} := \left(C_{i_0-1} \xrightarrow{\partial_{i_0-1}} C_{i_0} \xrightarrow{\partial_{i_0}} C_{i_0+1}\right)$, one can associate a CSS code C. Here, the homological degree i_0 is actually irrelevant since one can harmlessly shift globally the degrees; as a matter of fact, we shall assume hereinafter that $i_0 = 0$.

Proposition 1.15. *If* $\mathscr{C}$ *is a* 3*–length piece of based chain complex* $\mathscr{C} := \left(C_{-1} \xrightarrow{\partial_{-1}} C_0 \xrightarrow{\partial_0} C_1\right)$ *and* C *is the associated CSS code, then* C *has parameters* $[\![n_{\mathscr{C}}, k_{\mathscr{C}}, \min(d_{\mathscr{C}}, d_{\mathscr{C}^*}), \max(w_{\mathscr{C}}, w_{\mathscr{C}^*})]\!]$.

This statement can be regarded as folklore, but since it is central in our perspective and that it builds a bridge between two seemingly distant notions, we provide here a proof.

Proof. We set $\mathbf{H}_X := \mathrm{Mat}_{\mathcal{B}}(\partial_0)$ and $\mathbf{H}_Z := {}^t\mathrm{Mat}_{\mathcal{B}}(\partial_{-1})$. Since $\partial^2 = 0$, we have that $\mathbf{H}_X\,{}^t\mathbf{H}_Z = 0$ and the matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ define the CSS code C. Its length is $\dim(C_{i_0}) = n_{\mathscr{C}}$, its weight $\max(w_{\mathscr{C}}, w_{\mathscr{C}^*})$ and its dimension

$$\begin{aligned} n_{\mathscr{C}} - \mathrm{rk}(\mathbf{H}_X) - \mathrm{rk}(\mathbf{H}_Z) &= \dim(C_0) - \mathrm{rk}(\partial_0) - \mathrm{rk}(\partial_{-1}) \\ &= \dim\left(\mathrm{Ker}(\partial_0)\right) - \mathrm{rk}(\partial_{-1}) \\ &= \dim\left(\mathrm{Ker}(\partial_0)/\mathrm{Im}(\partial_{-1})\right) = \dim\left(H_0(\mathscr{C})\right) = k_{\mathscr{C}}. \end{aligned}$$

To compute the minimum distance, we consider an error E which commutes with every element of G but which is not in G. If E only involves Z alterations, then it can be described by a vector $v_E \in \mathbb{F}_2^n$ and the weight of E is $|v_E|$. Since E commutes with all the generators of G induced by the rows of $\mathbf{H}_X$, the vector v_E is orthogonal to all these rows and $v_E \in \mathrm{Ker}(\partial_0)$. But $E \notin G$, so v_E is not spanned by rows of $\mathbf{H}_Z$ and $v_E \notin \mathrm{Im}(\partial_{-1})$. It follows that E is non detectible iff $[v_E]$ is non zero in $H_0(\mathscr{C})$. If E only involves X alterations, then a similar reasoning at the dual level shows that E is non detectible iff $[v_E]$ is non zero in $H^0(\mathscr{C}) = H_0(\mathscr{C}^*)$. Now, for a general E, we factorize it as a product E_XE_Z where E_X and E_Z involves, respectively, only X and Z–alterations. Since every given generator of G involves only X alterations or only Z ones, the fact that E commutes with them implies that E_X and E_Z do. But $E \notin G$, so at least one of E_X or E_Z is not in G. We conclude by noting that the weight of E is greater than each of the weights of E_X and E_Z. □

Actually, classical error-correcting codes can also be interpreted as 2–length chain complexes. Indeed, if $\mathcal{C}$ is a classical code given by a parity check map $p_{\mathcal{C}} : E \twoheadrightarrow B$, then setting $C_0 := E$, $C_1 := B$ and $\partial_0 := p_{\mathcal{C}}$ defines a 2–length chain complex $\mathscr{C}$ such that $n_C = n_{\mathscr{C}}$, $k_C = k_{\mathscr{C}}$, $d_C = d_{\mathscr{C}}$ and $w_C = w_{\mathscr{C}}$. And by setting furthermore $C_{-1} := \{0\}$, $\mathcal{C}$ can also be seen as a CSS code C; it is however a very poor CSS code since $d_{\mathscr{C}^*} = 1$, and hence $d_C = \min(d_{\mathscr{C}}, d_{\mathscr{C}^*}) = 1$, whatever efficient $\mathcal{C}$ is. Poor, but not uninteresting, as we shall see in section 3.1.

It has already been noted that a CSS code can be interpreted as two orthogonal classical codes; this can now be reformulated, up to duality, as a classical code $\mathcal{C}_1$—defined by a parity-check map $p_{\mathcal{C}_1} := \partial_0 : C_0 \to C_1$—considered up to another classical code $\mathcal{C}_{-1} \subset \mathcal{C}_1$—defined by a generating map $g_{\mathcal{C}_{-1}} := \partial_{-1} : C_{-1} \to C_0$. It is then easily observed that $n_C = n_{\mathcal{C}_1} = n_{\mathcal{C}_{-1}}\left(= n_{\mathcal{C}_1^*} = n_{\mathcal{C}_{-1}^*}\right)$, $k_C = k_{\mathcal{C}_1} - k_{\mathcal{C}_{-1}}\left(= k_{\mathcal{C}_{-1}^*} - k_{\mathcal{C}_1^*}\right)$,

$w_C = \max(w_{C_1}, w_{C_{-1}^*})$ and, more interestingly, $d_C \geq \min(d_{C_1}, d_{C_{-1}^*})$. It may happen that all minimally weighted non trivial elements in C_1 are actually in C_{-1}; then they are not taken into account in d_C. We say that C have *quantum degeneracy* if $d_C > \min(d_{C_1}, d_{C_{-1}^*})$ or, equivalently, if $d_C > \min(d_{C_{-1}}, d_{C_1^*})$.

2 Tensor products for quantum codes

As we have seen in the previous section, 3–length chain complexes and CSS codes are two perspectives on the same object. Three operations were defined on the former: a dual operation, a direct sum and a tensor product. It is obviously tempting to transport them to the latter. Duality corresponds simply to the swap of $\mathbf{H}_X$ and $\mathbf{H}_Z$, and direct sum leads to the standard notion of CSS codes sum. We shall now focus on the tensor product.

2.1 Definitions

The tensor product on chain complexes has two drawbacks with regard to the CSS code point of view:

- it does not preserve the length of chain complexes, so that a rough product of two CSS codes is generally 5–length 5 instead of 3–length;
- it shuffles the homology groups of all degrees, so the resulting homology in degree 0 can generally not be determined by the input homologies in degree 0 only; this actually tends to increase the resulting dimension, but it is also fatal for the control of the resulting minimum distance.

We shall hence define first a notion of reduced chain complex to circumvent this obstacles.

2.1.1 Reduced chain complex

Definition 2.1. A chain complex $\mathscr{C}$ is said to be a *short complex* if its support is contained in $\{-1, 0, 1\}$. It is also said to be *balanced* if it has non trivial homology only in degree zero. A balanced short complex is said to be *reduced*. We finally say that $\mathscr{C}$, given with a basis $\mathcal{B}$, is *honest* if it is reduced and if neither $\mathrm{Mat}_{\mathcal{B}}(\partial_0)$ nor ${}^t\mathrm{Mat}_{\mathcal{B}}(\partial_{-1})$ has a column of zeros. Finally, we say that a CSS code C is *reduced* or *honest* if $\mathscr{C}$ is.

For a CSS code C, being reduced but not honest is something one should avoid. Indeed, up to duality, it means that one of the generator g of C_0 is in the kernel of ∂_0; then either g is also in the image of ∂_{-1}, but then $\mathscr{C}$ contains a useless direct summand of the form $\mathrm{Span}(\widetilde{g}) \hookrightarrow \mathrm{Span}(g) \twoheadrightarrow \{0\}$, where $\widetilde{g}$ is the unique preimage of g by ∂_{-1}, and this summand can be removed without altering the minimum distance, or it is not in the image of ∂_{-1}, but then the minimum distance is drastically pulled down to 1. Fortunatly, it is very easy to check whether a given short complex is honest or not.

Note that, by definition, a short complex has the following form: $C_{-1} \xrightarrow{\partial_{-1}} C_0 \xrightarrow{\partial_0} C_1$. So, in particular, its homology groups in degree -1 and 1 are, respectively $\mathrm{Ker}(\partial_{-1})$ and $\mathrm{Coker}(\partial_0)$, so it is reduced if and only if ∂_{-1} is injective and ∂_0 is surjective, that is if it has the form $C_{-1} \hookrightarrow C_0 \twoheadrightarrow C_1$. This is equivalent to requiring that $\dim\left(H_0(\mathscr{C})\right) = \dim(C_0) - \dim(C_{-1}) - \dim(C_1)$.

Any chain complex $\mathscr{C}$ can be turned into a short one by truncating the degrees higher than 1 and lower than -1. This operation obviously preserve the parameters of the chain complexe, but the result is generally not balanced, even if $\mathscr{C}$ was. The most natural and canonical way to adjust this is to consider

$$\mathrm{Ker}(\partial_{-1}) \hookrightarrow C_{-1} \xrightarrow{\partial_{-1}} C_0 \xrightarrow{\partial_0} C_1 \twoheadrightarrow \mathrm{Coker}(\partial_0) .$$

But beside its slightly overwidth support, it has also the disadvantage that none of $\mathrm{Ker}(\partial_{-1})$ or $\mathrm{Coker}(\partial_0)$ is naturally based, even if $\mathscr{C}$ is. One can, of course, pick randomly a basis, and this choice will have no consequence on the parameters of the resulting based chain complex, which are the same than those of $\mathscr{C}$, but it will have some effects on the parameters obtained after tensor products. For the sake of completeness, we do mention this canonical balancing process, but as soon as one is ready to get non canonical, the reduction process described in the next paragraph will eventually end with better parameters.

If $\mathscr{C}$ is given with a basis $\mathcal{B}$, then ∂_{-1} being non injective means that $\mathrm{Mat}_{\mathcal{B}}(\partial_{-1})$ contains some redundant columns. Similarly, ∂_0 being non surjective means that $\mathrm{Mat}_{\mathcal{B}}(\partial_0)$ contains some redundant rows. By truncating $\mathscr{C}$, removing a maximal set of such redundant columns and/or rows and modifying accordingly C_{-1} and C_1, one obtain a reduced chain complex which is easily seen to have the same paramaters than $\mathscr{C}$, except the weight which may even decrease if the rows with maximal weight were all redundant and removed. At the linear algebra level, C_{-1} is replaced by a complement space for $\mathrm{Ker}(\partial_{-1})$ spanned by vectors of $\mathcal{B}$, and C_1 by its quotient under a complement space of $\mathrm{Im}(\partial_0)$ spanned by vectors of $\mathcal{B}$. This process is however non canonical since it requires the choice of complement spaces, that is the choice of the redundant columns and rows to be removed.

Notation 2.2. For every chain complex $\mathscr{C}$, we shall denote

- by $\mathscr{C}_t$ its truncation to degrees -1, 0 and 1;
- by $\mathscr{C}_r$ the result of the reduction process applied to $\mathscr{C}_t$.

Note however that $\mathscr{C}_r$ is an abuse of notation since it depends on several choices made during the reduction process, but these choices can actually be made algorithmic by searching redundant—or, even better, maximally weighted redundant—columns or rows in a given order. Note also that if $\mathscr{C}$ is based, then so are $\mathscr{C}_t$ and $\mathscr{C}_r$.

2.1.2 Tensor products for CSS codes

Let C and $\mathcal{D}$ be two CSS codes. The most direct way to define a tensor product for C and $\mathcal{D}$ is to consider the CSS code associated to $(\mathscr{C} \otimes \mathscr{D})_t$. This would have terrible consequences on the resulting minimum distance if $\mathscr{C}$ and $\mathscr{D}$ were not balanced. And even if they are, the same consequences would arise for higher tensor powers. This motivates not only the following definitions, but it also justifies why we shall then give a non iterative definition for non reduced tensor powers.

Definition 2.3. For every CSS codes C and $\mathcal{D}$, we define

- $C \otimes \mathcal{D}$ as the CSS code associated to $\left(\mathscr{C} \otimes \mathscr{D}\right)_t$;
- $C \otimes_r \mathcal{D}$ as the CSS code associated to $\left(\mathscr{C} \otimes \mathscr{D}\right)_r$.

We shall also write $\otimes_{(r)}$ when denoting either $\otimes$ or $\otimes_r$.

One can note that, unlike for chain complexes and because of the truncation, $\otimes$ on CSS codes is not anymore an associative operation: one can compute that for three CSS codes C, $\mathcal{D}$ and $\mathcal{E}$, C_1 is involved in the degree -1 part of (the chain complex associated to) $(C \otimes \mathcal{D}) \otimes \mathcal{E}$ but not in the degree -1 part of $C \otimes (\mathcal{D} \otimes \mathcal{E})$.The reduced product $\otimes_r$ is not associative neither, because of all the choices made during the reduction processes.

Definition 2.4. For every CSS code $\mathscr{C}$ and every $\ell \in \mathbb{N}^*$, we define

- $C^{\otimes \ell}$ as the CSS code associated to $\left(\mathscr{C}^{\otimes \ell}\right)_t$;
- $C^{\otimes_r \ell}$ as the CSS code $\left(\cdots\left(\left(C \otimes_r C\right) \otimes_r C\right) \cdots \otimes_r C\right)$.

2.2 Properties

2.2.1 Lenghts, dimensions and weights for tensor products

Using Proposition 1.14, one can easily determine most of the parameters of $C \otimes \mathcal{D}$ and $C \otimes_r \mathcal{D}$, depending on those of $\mathscr{C}$ and $\mathscr{D}$.

Proposition 2.5. *If C and $\mathcal{D}$ are CSS codes, then*

- $n_{C\otimes\mathcal{D}} = n_{C\otimes_r\mathcal{D}} = n^{\mathscr{C}}_{-1}n^{\mathscr{D}}_1 + n^{\mathscr{C}}_0 n^{\mathscr{D}}_0 + n^{\mathscr{C}}_1 n^{\mathscr{D}}_{-1}$;
- $k_{C\otimes\mathcal{D}} = k_{C\otimes_r\mathcal{D}} = k^{\mathscr{C}}_{-1}k^{\mathscr{D}}_1 + k^{\mathscr{C}}_0 k^{\mathscr{D}}_0 + k^{\mathscr{C}}_1 k^{\mathscr{D}}_{-1}$;
- $d_{C\otimes\mathcal{D}} = d_{C\otimes_r\mathcal{D}} \leq \min\left(d^{\mathscr{C}}_{-1}d^{\mathscr{D}}_1, d^{\mathscr{C}}_0 d^{\mathscr{D}}_0, d^{\mathscr{C}}_1 d^{\mathscr{D}}_{-1}, d^{\mathscr{C}^*}_{-1} d^{\mathscr{D}^*}_1, d^{\mathscr{C}^*}_0 d^{\mathscr{D}^*}_0, d^{\mathscr{C}^*}_1 d^{\mathscr{D}^*}_{-1}\right)$;

- $w_{C\otimes\mathcal{D}} = \max\left(w^{\mathscr{C}}_{-1} + w^{\mathscr{D}}_{1}, w^{\mathscr{C}}_{0} + w^{\mathscr{D}}_{0}, w^{\mathscr{C}}_{1} + w^{\mathscr{D}}_{-1}, w^{\mathscr{C}^*}_{-1} + w^{\mathscr{D}^*}_{1}, w^{\mathscr{C}^*}_{0} + w^{\mathscr{D}^*}_{0}, w^{\mathscr{C}^*}_{1} + w^{\mathscr{D}^*}_{-1}\right)$;
- $w_{C\otimes_r\mathcal{D}} \leq \max\left(w^{\mathscr{C}}_{-1} + w^{\mathscr{D}}_{1}, w^{\mathscr{C}}_{0} + w^{\mathscr{D}}_{0}, w^{\mathscr{C}}_{1} + w^{\mathscr{D}}_{-1}, w^{\mathscr{C}^*}_{-1} + w^{\mathscr{D}^*}_{1}, w^{\mathscr{C}^*}_{0} + w^{\mathscr{D}^*}_{0}, w^{\mathscr{C}^*}_{1} + w^{\mathscr{D}^*}_{-1}\right)$.

It should be noted that the parameters of tensor products does not depend on the parameters of input CSS codes, but on those of the underlying chain complexes only. This can however be partially fixed when the CSS codes are reduced.

Proposition 2.6. *If C and $\mathcal{D}$ are reduced CSS codes, then*

- $n_{C\otimes\mathcal{D}} = n_{C\otimes_r\mathcal{D}} \leq n_C n_{\mathcal{D}} + (n_C - k_C)(n_{\mathcal{D}} - k_{\mathcal{D}})$;
- $k_{C\otimes\mathcal{D}} = k_{C\otimes_r\mathcal{D}} = k_C k_{\mathcal{D}}$.

We want to stress here that, despite appearances, the general upper bound for the minimum distances does not yield an upper bound $d_{C\otimes\mathcal{D}} \leq d_C d_{\mathcal{D}}$, even if C and $\mathcal{D}$ are reduced. We will see examples satisfying $d_{C\otimes\mathcal{D}} > d_C d_{\mathcal{D}}$ in section 3.1.

2.2.2 Bounds for minimum distances

Tensor products of CSS codes are useless if minimum distances can not be estimated; but Proposition 2.6 gives only an upper bound, which is more a constraint than a control. We give now a criterion which shall provide a lower bound. But, first, we need to introduce an additional definition. If Ω is a subset of a $\mathbb{F}_2$–space given with a basis $\mathcal{B}$, then we define

$$\mathrm{overlap}(\Omega) := \max_{b\in\mathcal{B}} \left| \left\{ p \in \Omega \;\middle|\; b \in p \right\} \right|.$$

If, using $\mathcal{B}$, one considers the elements of Ω as vectors and stacks them as the rows of a matrix, then $\mathrm{overlap}(\Omega)$ corresponds to the maximum weight of a column.

Definition 2.7. For any $N, K \in \mathbb{N}^*$, we say that a based chain complex $\mathscr{C}$ is (N, K)–*cocontrolled* if there exist a basis $[g_1^*], \ldots, [g_k^*]$ for $H^0(\mathscr{C})$ and, for every $i \in \{1, \ldots, k\}$, a set $\Omega_i \subset C_0^*$ of representatives for $[g_i^*]$ with $|\Omega_i| \geq N$ and $\mathrm{overlap}(\Omega_i) \leq K$.

We can now state the main result of this part, which is the following lemma:

Lemma 2.8 ([2, Lem. 2.7])**.** *Let $N, K \in \mathbb{N}^*$ and let $\mathscr{C}$ be a (N, K)–cocontrolled based chain complex. Then, for every chain complex $\mathscr{D}$ such that either $\mathscr{C}$ or $\mathscr{D}$ is balanced,*

$$d_{\mathscr{C}\otimes\mathscr{D}} \geq \left\lceil \frac{N}{K} d_{\mathscr{D}} \right\rceil.$$

This leads to the following statement for CSS codes:

Theorem 2.9 ([2, Th. 2.8])**.** *Let C be a reduced CSS code such that $\mathscr{C}$ and $\mathscr{C}^*$ are both (N, K)–cocontrolled with $N, K \in \mathbb{N}^*$. Then for all CSS code $\mathcal{D}$,*

$$d_{C\otimes\mathcal{D}}, d_{C\otimes_r\mathcal{D}} \geq \left\lceil \frac{N}{K} d_{\mathcal{D}} \right\rceil.$$

Remark 2.10. In fact, we will consider a basis $g_1, \ldots, g_r$ of $\mathrm{Ker}(\partial_0) \subset C_0$ such that the first elements induce a basis $[g_1], \ldots, [g_k]$ of $H_0(\mathscr{C})$ and look, for every $i_0 \in \{1, \ldots, k\}$, at linear forms in $\mathrm{Ker}(\partial_{-1}^*)$ which vanish on all g_i but g_{i_0} that is, using the scalar product isomorphism between C_0 and C_0^*, elements of C_0 which share an even number of generators with all g_i but g_{i_0}. As $H^0(\mathscr{C}^*) \cong H_0(\mathscr{C}) \cong H^0(\mathscr{C})^*$, we shall often restrict our attention on a basis for $H_0(\mathscr{C})$ and its dual. But if the chain complex $\mathscr{C}$ is symmetric, then it is sufficient to consider $\mathscr{C}$ since the same Ω–sets can be used again to handle $\mathscr{C}^*$.

Remark 2.11. Lemma 2.8 implies actually slightly stronger results since

1. the lower bounds for $d_{\mathscr{C}\otimes_{(r)}\mathscr{D}}$ and $d_{\mathscr{C}^*\otimes_{(r)}\mathscr{D}^*}$ can be handled independantly: one may focus on, say, $\mathscr{C}$ to work on $d_{\mathscr{C}\otimes_{(r)}\mathscr{D}}$ and on $\mathscr{D}^*$ for $d_{\mathscr{C}^*\otimes_{(r)}\mathscr{D}^*}$; this would lead to a lower bound of the form
$$d_{C\otimes\mathcal{D}}, d_{C\otimes_r\mathcal{D}} \geq \left\lceil \min\left(\frac{N_{\mathscr{C}}}{K_{\mathscr{C}}} d_{\mathscr{D}}, \frac{N_{\mathscr{D}^*}}{K_{\mathscr{D}^*}} d_{\mathscr{C}^*}\right)\right\rceil;$$
2. the CSS code C may not be reduced as soon as $\mathcal{D}$ is.

For instance, applying Lemma 2.8 with the reduced chain complex $\mathscr{D} := \{0\} \hookrightarrow \mathbb{F}_2 \twoheadrightarrow \{0\}$, we obtain the following result whose statement, oddly enough, does not involve any tensor product, and which gives a lower bound for the minimum distance of any CSS code, even not reduced:

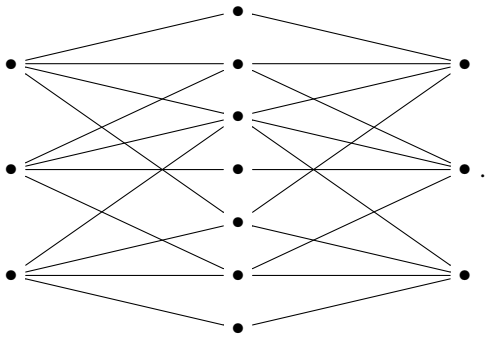
Corollary 2.12. *If C is a (possibly non reduced) CSS code such that $\mathscr{C}$ and $\mathscr{C}^*$ are both (N, K)–cocontrolled with $N, K \in \mathbb{N}^*$, then $d_{\mathscr{C}} \geq \left\lceil \frac{N}{K} \right\rceil$.*

However, most of the other applications will use only the statement of Theorem 2.9, and often in its one dimensional case, which is even simpler to state:

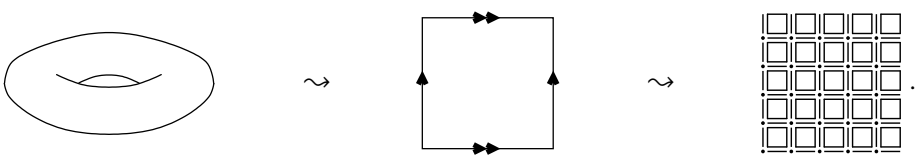
Corollary 2.13. *Let $N, K \in \mathbb{N}^*$ and let C be a reduced CSS code of dimension 1. If there exist two subsets, $\Omega \subseteq \mathrm{Ker}(\partial_0) \setminus \mathrm{Im}(\partial_{-1})$ and $\Omega' \subseteq \mathrm{Ker}(\partial^*_{-1}) \setminus \mathrm{Im}(\partial^*_0)$, with $|\Omega|, |\Omega'| \geq N$ and $\mathrm{overlap}(\Omega), \mathrm{overlap}(\Omega') \leq K$, then for all CSS code $\mathcal{D}$,*
$$d_{C\otimes\mathcal{D}}, d_{C\otimes_r\mathcal{D}} \geq \left\lceil \frac{N}{K} d_{\mathcal{D}} \right\rceil.$$

Examples 2.14.

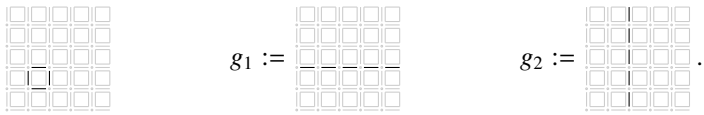
1. In its principal symmetric form, the Steane CSS code with parameter $[\![7, 1, 3]\!]$, that we shall denote by $\mathcal{S}_{7;1;3}$, has the following associated chain complex:



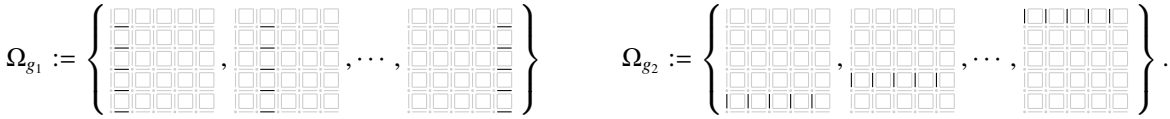
We denote the generators in degree 0, from top to bottom, by positive integers from 1 to 7. Using the subset identification to write down the results, it can be computed by hand that $\mathrm{Ker}(\partial_0) = \mathrm{Span}(1235, 2346, 3567, 124)$,that the homology is generated by $\{124\}$, and that $d_{\mathcal{S}_{7;1;3}\otimes_{(r)}\mathcal{S}_{7;1;3}} = 7$; this example was already considered in [BH13a, Section V.A] but for another notion of tensor product that will be discussed in Section 2.2.4. Using Corollary 2.12 and Theorem 2.9 with
$$\Omega_{124} := \big\{124, 136, 157, 237, 256, 345, 467\big\},$$
we actually obtain that $d_{\mathcal{S}_{7;1;3}} \geq \left\lceil \frac{7}{3} \right\rceil = 3$ and $d_{\mathcal{S}_{7;1;3}\otimes_{(r)}\mathcal{S}_{7;1;3}} \geq \frac{7}{3} d_{\mathcal{S}_{7;1;3}} = 7$. This is an example where Theorem 2.9 and Corollary 2.12 give sharp bounds whereas $\frac{N}{K} \notin \mathbb{N}$. We shall see in Section 3.3 a generalization of $\mathcal{S}_{7;1;3}$.
2. In [Kit03], A. Kitaev defined his eponymous CSS codes $\mathcal{K}_n$ by considering the chain complex associated to the $(n \times n)$–grid cell decomposition of the torus:



Bases for C_{-1}, C_0 and C_1 are respectively given by squares, segments and dots, and maps are given as the boundary maps. It is well-known that the resulting code has parameters $[\![2n^2, 2, n, 4]\!]$. Indeed, it is easily seen that all the homologically trivial elements of $\mathrm{Ker}(\partial_0)$ are generated by small squares and non trivial ones by any vertical and any horizontal lines:



This shows that $d_{\mathcal{K}_n} \leq n$ and the converse inequality can be proven using Corollary 2.12 with



Theorem 2.9 can be applied with unit sets for the Ω's and the Ω''s, it leads to a rougher but more general lower bound:

Corollary 2.15. *If C and $\mathcal{D}$ are two CSS codes and one of them is reduced, then $d_{C\otimes\mathcal{D}}, d_{C\otimes_r\mathcal{D}} \geq \max(d_C, d_{\mathcal{D}})$.*

This lowed bound was more or less predicted, but an unexpected corollary of Theorem 2.9 is that, except in some trivial cases, this bound is never sharp. Indeed, having a closer look at the overlaps of the Ω's, we obtain:

Corollary 2.16 ([2, Cor. 2.18])**.** *If C and $\mathcal{D}$ are two honest CSS codes, then $d_{C\otimes\mathcal{D}}, d_{C\otimes_r\mathcal{D}} \geq 2\max(d_C, d_{\mathcal{D}})$.*

As we will see at the end of the next section, this additional 2 factor has major consequences on the generic behavior of iterated powers.

Unfortunately, we shall end this section by a lemma which kills all hope that one may have to use the above "$\frac{N}{K}$"–criterion to exhibit an LDPC family of CSS codes with minimum distance growing faster than the square root of the lengths.

Lemma 2.17 ([2, Rk. 2.13])**.** *If $\mathscr{C}$ is (N, K)–cocontrolled, then $\frac{N}{K} d_{\mathscr{C}^*} \leq n_{\mathscr{C}}$.*

Compared with Corollary 2.12, it follows in particular that, if the minimum distance of a CSS code C can be well approached by such a (N, K)–cocontrol, then $d_C \lesssim \sqrt{n_C}$.

2.2.3 Parameters for iterated tensor powers

Considering the tensor powers of a given CSS code produces an infinite family of codes which is naturally LDPC. We will now estimate the asymptotical parameters of such a family. Note that, to make the formulae less cluttered, we shall omit $\mathscr{C}$ in the n_i–notation of the next two propositions.

Proposition 2.18 ([2, Cor. 2.20])**.** *Let C be a reduced CSS code. If $\mathscr{C}$ and $\mathscr{C}^*$ are both (N, K)–cocontrolled with $N, K \in \mathbb{N}^*$, then $\left(C^{\otimes\ell}\right)_{\ell\in\mathbb{N}}$ is a family of CSS codes with parameters*

$$\left[\!\!\left[\sim \frac{1}{2}\sqrt{\frac{n_0 + 2\sqrt{n_{-1}n_1}}{\pi\ell\sqrt{n_{-1}n_1}}}\left(n_0 + 2\sqrt{n_{-1}n_1}\right)^\ell \ , \ (n_0 - n_{-1} - n_1)^\ell \ , \geq \left(\frac{N}{K}\right)^\ell \ , \leq n_0\ell \right]\!\!\right].$$

In particular, the family is LDPC and the minimum distance grows strictly faster than the $\frac{\log(n_0+2\sqrt{n_{-1}n_1})}{\log(N)-\log(K)}$-th power of the length.

Proposition 2.19 ([2, Prop. B.1])**.** *Let C be a reduced CSS code. If $\mathscr{C}$ and $\mathscr{C}^*$ are both (N,K)–cocontrolled with $N,K\in\mathbb{N}^*$, then for every $\ell\in\mathbb{N}$, $\left(C^{\otimes_r\ell}\right)_{\ell\in\mathbb{N}}$ is a family of CSS codes with parameters*

$$\left[\!\!\left[m_\ell\ ,\ (n_0-2n_1)^\ell\ ,\ \geq\left(\frac{N}{K}\right)^\ell\ ,\ \leq n_0\ell\right]\!\!\right],$$

where, denoting respectively by n_a and n_r the additive and multiplicative means of n_{-1} and n_1,

$$m_\ell:=\frac{2n_r^2\left(n_0-2n_a\right)^\ell+\left(n_{-1}^2+2n_an_r+n_1^2\right)\left(n_0+n_r\right)^\ell+\left(n_{-1}^2-2n_an_r+n_1^2\right)\left(n_0-n_r\right)^\ell}{2\left(n_{-1}^2+n_r^2+n_1^2\right)};$$

which simplifies into $m_\ell=\frac{2}{3}\left((n_0+n_1)^\ell+(n_0-2n_1)^\ell\right)$ when $\mathscr{C}$ is symmetric. In particular, the family is LDPC and the minimum distance grows at least as the $\frac{\log(n_0+\sqrt{n_{-1}n_1})}{\log(N)-\log(K)}$-th power of the length.

Remark 2.20. In Propositions 2.18 and 2.19, the lower bounds $\left(\frac{N}{K}\right)^\ell$ for the minimum distances can be slighty improved into $\left\lceil\cdots\left\lceil\left\lceil\frac{N}{K}\right\rceil\frac{N}{K}\right\rceil\frac{N}{K}\cdots\right\rceil$ but, in fact, this only provides a better constant factor for the minimum distance growth.

Combined with Corollary 2.16, Propositions 2.18 and 2.19 have the following consequence:

Corollary 2.21. *If C is an honest CSS code, then the families $\left(C^{\otimes\ell}\right)_{\ell\in\mathbb{N}}$ and $\left(C^{\otimes_r\ell}\right)_{\ell\in\mathbb{N}}$ are LDPC with $d_{C^{\otimes\ell}},d_{C^{\otimes_r\ell}}\geq 2^\ell$ for every $\ell\in\mathbb{N}^*$.*

This has two remarkable outcomes:

- tensoring iteratively any honest CSS code C provides an LDPC family with minimum distance growing to infinity;
- even if C has no quantum degeneracy, its ℓ-th (reduced) tensor power, for some large enough ℓ, does. Indeed, it has been noticed that the weights, that is the maximal weigth for a row of $\mathrm{Mat}\left(\partial_0^{\mathcal{C}^{\otimes(r)^\ell}}\right)$ or ${}^t\mathrm{Mat}\left(\partial_{-1}^{\mathcal{C}^{\otimes(r)^\ell}}\right)$, grow at most linearly with ℓ; but the same is true for the columns of $\mathrm{Mat}\left(\partial_{-1}^{\mathcal{C}^{\otimes(r)^\ell}}\right)$ or ${}^t\mathrm{Mat}\left(\partial_0^{\mathcal{C}^{\otimes(r)^\ell}}\right)$, and this provides an upper bound for the minimum distance of the classical codes $\mathrm{Im}\left(\partial_{-1}^{\mathcal{C}^{\otimes(r)^\ell}}\right)$ and $\mathrm{Im}\left(\partial_0^{*\mathcal{C}^{\otimes(r)^\ell}}\right)$ which grow hence at most linearly with ℓ. These classical minimum distances are hence eventually bitten by $d_{C^{\otimes(r)^\ell}}$ which grows exponentially with ℓ.

2.2.4 Connection with Bravyi–Hasting homological product

In [BH14], Bravyi and Hastings introduced another notion of homological product for CSS codes, that we will denote here by $\boxtimes$. In their framework, they do not consider general chain complexes, but only 2–nilpotent maps; this data is indeed sufficient to get a composition of maps which is zero, and hence to get a CSS code. As we shall see, Bravyi and Hastings' product $\boxtimes$ is closely related to $\otimes$.

Definition 2.22. Let C,D be two $\mathbb{F}_2$–spaces, and $\partial_C\in\mathrm{End}(C),\partial_D\in\mathrm{End}(D)$ be two 2–nilpotent maps. We define their *homological product* as the 2–nilpotent map

$$\partial_C\boxtimes\partial_D:=\partial_C\otimes\mathrm{Id}_D+\mathrm{Id}_C\otimes\partial_D\in\mathrm{End}(C\otimes D).$$

If C and $\mathcal{D}$ are the CSS codes associated to, respectively, ∂_C and ∂_D, then we define $C\boxtimes\mathcal{D}$ as the CSS code associated to $\partial_C\boxtimes\partial_D$.

Proposition 2.23 ([BH14])**.** *If C and $\mathcal{D}$ are two CSS codes described by 2–nilpotent maps, then $k_{C\boxtimes\mathcal{D}}=k_Ck_\mathcal{D}$ and $\max(d_C,d_\mathcal{D})\leq d_{C\boxtimes\mathcal{D}}\leq d_Cd_\mathcal{D}$.*

Bravyi and Hastings show moreover that for a random CSS code C of length n, the minimum distance of $C \boxtimes C$ is larger than cn^2 for some positive constant c with a probability tending to 1 when n tends to infinity.

Now, let C and $\mathcal{D}$ be two CSS codes described by 2–nilpotent maps $\partial_C \in \mathrm{End}(C)$ and $\partial_D \in \mathrm{End}(D)$. From the chain complex point of view, C is actually the CSS code associated to

$$\widetilde{\mathscr{C}} := \; C \xrightarrow{\partial_C} C \xrightarrow{\partial_C} C \; ,$$

which can be reduced into

$$\mathscr{C} := \; C_- \xhookrightarrow{\partial_C} C \xrightarrow{\partial_C} C_+ \; ,$$

where $C =: C_- \oplus \mathrm{Ker}(\partial_C)$ and $C_+ := C/C'_+$ with $C := C'_+ \oplus \mathrm{Im}(\partial_C)$. We set similar notation for $\mathcal{D}$. As explicitly shown in [2, Sec. 2.2.5], $\mathscr{C} \otimes \mathscr{D}$ can be decomposed into an direct sum $\mathscr{P}_1 \oplus \mathscr{P}_2 \oplus \mathscr{P}_3$ where $\mathscr{P}_1$ and $\mathscr{P}_3$ are acyclic, and $\mathscr{P}_2$ is isomorphic, as a chain complex, to

$$C \otimes D_- + C_- \otimes D \xrightarrow{\mathrm{Id}_C \otimes \partial_D + \partial_C \otimes \mathrm{Id}_D} C \otimes D \xrightarrow{\mathrm{Id}_C \otimes \partial_D + \partial_C \otimes \mathrm{Id}_D} C \otimes D/C'_+ \otimes D'_+ \; ,$$

which is a partially reduced form of the chain complex associated to $\partial_C \boxtimes \partial_D$. As a consequence, we obtain that $H(\partial_C \boxtimes \partial_D) \cong H_0(\mathscr{C} \otimes \mathscr{D}) \cong H_0(\mathscr{C}) \otimes H_0(\mathscr{D}) \cong H(\partial_C) \otimes H(\partial_D)$. The homological product can be hence seen as a subcomplex of the tensor product that contains all the homology. This provides a substantial reduction of the length, $n_0^{\mathscr{C}} n_0^{\mathscr{D}}$ instead of $n_{-1}^{\mathscr{C}} n_1^{\mathscr{D}} + n_0^{\mathscr{C}} n_0^{\mathscr{D}} + n_1^{\mathscr{C}} n_{-1}^{\mathscr{D}}$, but the variation of the minimum distance is, again, more difficult to estimate. However, the mimimum distances are very likely to behave similarly with both notion of product, and actually, the criterion provided for $\otimes$ in Theorem 2.9 and all its consequences hold also true for $\boxtimes$. Indeed, a close look at the proof of Lemma 2.8 shows that the isomorphism between $\mathscr{P}_2$ and the partially reduced form of $\partial_C \boxtimes \partial_D$ preserves the lower bound on the minimum distance, implying then the following statements:

Theorem 2.24 ([2, Th. 3.10])**.** *Let C be a CSS code defined by a 2–nilpotent map ∂. Let $g_1, \ldots, g_r$ be a basis for $\mathrm{Ker}(\partial)$ such that $g_1, \ldots, g_k$ induce a basis for $\mathrm{Ker}(\partial)/\mathrm{Im}(\partial)$. If, for any $i \in \{1, \ldots, k\}$, there exists $\Omega_i \subseteq g_i^* + \mathrm{Im}(\partial^*)$ and $\Omega'_i \subseteq g_i + \mathrm{Im}(\partial)$, with $|\Omega_i|$, $|\Omega'_i| \geq N$ and $\mathrm{overlap}(\Omega_i)$, $\mathrm{overlap}(\Omega'_i) \leq K$; then, for any CSS code $\mathcal{D}$ defined by a 2–nilpotent map, we have*

$$d_{C \boxtimes \mathcal{D}} \geq \left\lceil \frac{N}{K} d_{\mathcal{D}} \right\rceil .$$

Corollary 2.25 ([2, Cor. 3.11])**.** *If C and $\mathcal{D}$ are CSS codes described by 2–nilpotent matrices which have no column nor row of zeros, then $d_{C \boxtimes \mathcal{D}} \geq 2 \max(d_C, d_{\mathcal{D}})$.*

Conversely, forgetting its grading turns any chain complex into a 2–nilpotent map. We explain now how the tensor product of two chain complexes can be extracted from the homological product of the associated 2–nilpotent maps. Recall that every chain complex $\mathscr{C}$ is underlain by an $\mathbb{F}_2$–space $C := \bigoplus_{i \in \mathbb{Z}} C_i$ and a 2–nilpotent map $\partial_C := \bigoplus_{i \in \mathbb{Z}} \partial_i$. It is easily checked that $\mathrm{Ker}(\partial_C)/\mathrm{Im}(\partial_C) = H_\bullet(\mathscr{C}) := \bigoplus_{i \in \mathbb{Z}} H_i(\mathscr{C})$. In particular, $\ker(\partial_C)/\mathrm{Im}(\partial_C) \cong H_0(\mathscr{C})$ whenever $\mathscr{C}$ is balanced. Then, if $\mathscr{C}$ and $\mathscr{D}$ are two reduced complexes, $C \otimes D \xrightarrow{\partial_C \boxtimes \partial_D} C \otimes D \xrightarrow{\partial_C \boxtimes \partial_D} C \otimes D$ decomposes into the direct sum $\bigoplus_{i \in \mathbb{Z}} \left\{\mathscr{C} \otimes \mathscr{D}\right\}_i$, where $\left\{\mathscr{C} \otimes \mathscr{D}\right\}_i$ is the 3–length truncature of $\mathscr{C} \otimes \mathscr{D}$ centered in degree i. They all have null homology except the summand $i = 0$ which actually correponds to $(\mathscr{C} \otimes \mathscr{D})_t$. Moreover, any basis induced from bases on $\mathscr{C}$ and $\mathscr{D}$ respects this direct sum decomposition; all $\left\{\mathscr{C} \otimes \mathscr{D}\right\}_i$ with $i \neq 0$ are hence acyclic direct summands which can be harmlessly removed. It follows that $k_{\mathscr{C} \boxtimes \mathscr{D}} = k_{\mathscr{C} \otimes \mathscr{D}}$ and $d_{\mathscr{C} \boxtimes \mathscr{D}} = d_{\mathscr{C} \otimes \mathscr{D}}$. Besides, it is easily checked that $n_{\mathscr{C} \boxtimes \mathscr{D}} = \left(\sum_i n_i^{\mathscr{C}}\right)\left(\sum_i n_i^{\mathscr{D}}\right)$. In particular, if $\mathscr{C}$ is a based reduced complex, the iterated powers $C^{\boxtimes \ell}$, $C^{\otimes \ell}$ and $C^{\otimes_r \ell}$ have same dimensions and same minimum distances, but differents lengths, which are respectively $(n_{-1} + n_0 + n_1)^\ell$, $O\left(\frac{(n_0 + 2\sqrt{n_{-1} n_1})^\ell}{\sqrt{\ell}}\right)$ and $O\left((n_0 + \sqrt{n_{-1} n_1})^\ell\right)$.

In conclusion, there are two natural notions of product for CSS codes, namely tensor and homological ones, and it is easy to switch from one to the other. They both generate LDPC families when used iteratively and it is natural to question whether a construction is better than the other. The answer is actually negative and, as we summarize below, the qualities of the iterated tensor or homological powers depend on the initial nature of the input code:

- *if the input code is described by a* 2*–nilpotent map*, then one can see it as a chain complex with repeated space and map; but the homological powers of the original 2–nilpotent map provide shorter codes with same dimensions than the tensoriel powers. Moreover, the control of the minimum distances provided by the present dissertation is equal for both;
- *if the input code is described by a chain complex*, then one can consider the underlying 2–nilpotent map by forgetting the grading; but the tensor powers of the original chain complex provide shorter codes with same dimensions and minimum distances, hence better relative parameters, than the homological powers.

3 Families of CSS codes

We now switch to applications of Theorem 2.9 for the construction of LDPC families of CSS codes, with a special focus on the growth speed of minimum distances compared to the lengths.

3.1 Tillich–Zemor codes

The theory of error-correcting codes can be seen as the theory of shuffling the canonical basis of a genuine injection, $\mathbb{F}_2^k \hookrightarrow \mathbb{F}_2^n$ or $\mathbb{C}^{2^k} \hookrightarrow \mathbb{C}^{2^n}$ where $k < n$, so that the minimum distances get as close to n as possible. As shown by their long-studied theory, this can be reasonably achieved for classical codes. But what makes quantum codes much more intricate is that the minimum distances of C involves simultaneously the minimum distances of $\mathscr{C}$ and $\mathscr{C}^*$, and an artificial increase of $d_{\mathscr{C}}$ often leads to a critical decrease for $d_{\mathscr{C}^*}$. Nonetheless, tensor products offer a way to take anyway advantage of CSS codes which has low minimum distances because of such an imbalance between $d_{\mathscr{C}}$ and $d_{\mathscr{C}^*}$. Indeed, it follows from Proposition 2.18 that, for reduced CSS codes C and $\mathcal{D}$, $d_{C\otimes\mathcal{D}}$ and $d_{C\otimes,\mathcal{D}}$ are bounded above by the minimum between $d_{\mathscr{C}}d_{\mathscr{D}}$ and $d_{\mathscr{C}^*}d_{\mathscr{D}^*}$. An important fact is that none of $d_{\mathscr{C}}d_{\mathscr{D}^*}$ or $d_{\mathscr{C}^*}d_{\mathscr{D}}$ is involved in this upper bound; one can hence tensorize such imbalanced CSS codes so that the weak leg of one is tamed by the strong one of the other. Initially based on a graph point of view, Tillich–Zemor codes, defined in [TZ14] can be interpreted as an occurence of such a phenomenon.

Indeed, as explained at the end of Section 1.3.3, a classical code $\mathcal{C}$ described by a parity-check matrix provides a CSS code C with $n_C = n_{\mathcal{C}}$, $k_C = k_{\mathcal{C}}$ and $d_C = \min(d_{\mathscr{C}}, d_{\mathscr{C}^*}) = \min(d_{\mathcal{C}}, 1) = 1$. From a dual perspective, a classical code $\mathcal{D}$ described by a generating matrix also provides a CSS code $\mathcal{D}$ with $n_{\mathcal{D}} = n_{\mathcal{D}^\perp}$, $k_{\mathcal{D}} = k_{\mathcal{D}^\perp}$ and $d_{\mathcal{D}} = \min(d_{\mathscr{D}}, d_{\mathscr{D}^*}) = \min(1, d_{\mathcal{D}^\perp}) = 1$. Combining these observations with Corollary 2.15 refined in the light of the first point of Remark 2.11, we can reformulate[3] Tillich and Zemor's result as:

Theorem 3.1 ([TZ14])**.** *If $\mathcal{C}$ and $\mathcal{D}$ are two classical codes given, respectively, by a generating map $g_{\mathcal{C}}$ and a parity-check map $p_{\mathcal{D}}$, then the CSS code $C \otimes \mathcal{D}$ associated to* $\left(C_{-1} \xhookrightarrow{g_{\mathcal{C}}} C_0 \right) \otimes \left(D_0 \xrightarrow{p_{\mathcal{D}}} D_1 \right)$ *has parameters $n_{C\otimes\mathcal{D}} = n_{\mathcal{C}^\perp} n_{\mathcal{D}} + (n_{\mathcal{C}^\perp} - k_{\mathcal{C}^\perp})(n_{\mathcal{D}} - k_{\mathcal{D}})$, $k_{C\otimes\mathcal{D}} = k_{\mathcal{C}^\perp} k_{\mathcal{D}}$, $d_{C\otimes\mathcal{D}} = \min(d_{\mathcal{C}^\perp}, d_{\mathcal{D}})$ and $w_{C\otimes\mathcal{D}} = \max\left(w_{\mathcal{C}^\perp} + w_{\mathcal{D}}, w_{\mathcal{C}^\perp} + w_{\mathcal{D}}\right)$.*

We stress here the fact that $C_{-1} \xhookrightarrow{g_{\mathcal{C}}} C_0$ and $D_0 \xrightarrow{p_{\mathcal{D}}} D_1$ are reduced but not honest, so Corollary 2.15 applies —and, actually, leads to an equality— but Corollary 2.16 does not. Applied to LDPC classical codes, whose dimensions and minimum distances are linear in the lengths [Gal62], Theorem 3.1 leads to LDPC families of CSS codes with dimensions linear in the lengths and minimum distances growing as the square root of the lengths.

[3] the relationship between Tillich–Zemor hypergraph and homological product was already notified in [FH14]

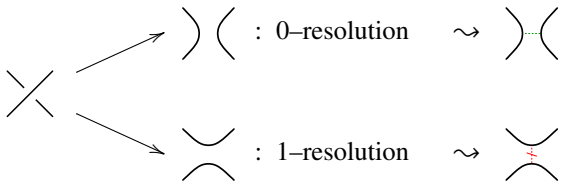
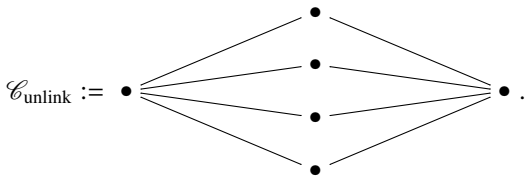


Figure II.1: Canonical resolutions for a crossing and their markings

3.2 Khovanov codes

The simplest symmetric honest complex is:

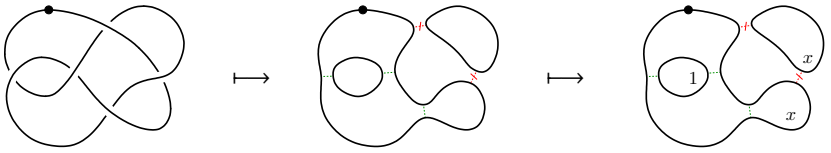


If denoting the generators in degree 0, from top to bottom, by positive integers from 1 to 4, and using the subset identification, then it can be easily computed that the homology is generated by 12 and 13. Applying Proposition 2.18 with $\Omega_{12} := \{24, 13\}$ and $\Omega_{13} := \{34, 12\}$, we obtain that the family of CSS codes $\left(C_{\text{unlink}}^{\otimes \ell}\right)_{\ell \in \mathbb{N}^*}$ has asymptotical parameters equal to $\left[\!\!\left[\sqrt{\frac{3}{2\pi\ell}} 6^\ell, 2^\ell, 2^\ell, 4\ell \right]\!\!\right]$. As its subscript name suggests, these CSS codes can actually be considered as examples of the "knot theory"-grounded Khovanov codes that we introduced in [10].

3.2.1 A brief construction of Khovanov chain complexes

Introduced by M. Khovanov in [Kho00], Khovanov homology is a link invariant which was the first example of categorification for a polynomial link invariant. Khovanov homology is indeed a bigraded homology theory defined for link whose graded Euler characteristic recovers Jones polynomial. Combinatorially defined from link diagrams, Khovanov homology produces chain complexes which naturally satisfy properties which are likely to bring interesting CSS codes. We shall now give a very brief overview of its construction. However, since we are only interested here in its application to CSS codes, we shall step back from the historical construction to focus on a simpler version which is less interesting for topological purpose but more adapted to CSS codes: we shall consider only the reduced version over $\mathbb{F}_2$ for non oriented pointed links and work with a non standard basis which actually do not respect the second grading. As a matter of fact we shall only mention this second grading and drop out some orientation-related global shift of the bigrading. We refer the interested reader to [Kho00, Kho03, Vir04, Tur17, Shu11] for more details.

Let D be a pointed link diagram with n crossings, which is a generic immersed curve in $\mathbb{R}^2$ with n transverse double points enhanced with an over/under information, and a marked point which is not one of the double points. A *resolution for a crossing of D* is a choice of smoothing which remove the double point; there are two canonical way to do it, shown in Figure II.1 and respectively called the *0* and the *1–resolution*. A *resolution for D* is a map $\phi\colon \{\text{crossings of } D\} \longrightarrow \{0, 1\}$, it can be pictured as the resolution diagram D_ϕ, obtained from D by $\phi(c)$–resolving every crossing c of D and adding markings to indicate the nature of the resolutions as on the rightmost column of Figure II.1. Note that resolution diagrams are *not* considered up to isotopies and distinct maps ϕ always lead to distinct resolution diagrams D_ϕ. Since it has no crossing anymore, D_ϕ is a union of disjoint circles embedded in the plane, and one of this circle is dotted by the marked point. An *enhanced resolution of D*, denoted by D_ϕ^σ, is a resolution D_ϕ of D together with a labeling map $\sigma\colon \{\text{circles of } D_\phi\} \longrightarrow \{1, x\}$ which sends the dotted circle to x; see Figure II.2 for an illustration. The labels can be seen as elements of $\mathbb{F}_2[x]/x^2$, and later, when dealing with combinations of enhanced



a diagram a resolution an enhanced resolution

Figure II.2: From diagrams to enhanced resolutions

diagrams, we shall assume multi-linearity for the labels: a resolution diagram with a circle labeled by a sum $a + b$ shall be then thought of as a sum of two resolution diagrams, one with the circle labeled by a and the other labeled by b; in particular, any 0 label on a circle shall make the whole resolution diagram equal to zero.

Now we define C_D as the $\mathbb{F}_2$–space spanned by enhanced resolutions and $\partial_D \in \mathrm{End}(C_D)$ by

$$\partial_D(D_\phi^\sigma) = \sum_{c \in \phi^{-1}(0)} \partial_c(D_\phi^\sigma)$$

where $\partial_c(D_\phi^\sigma)$ is a sum of enhanced resolutions over $D_{\phi+\delta_c}$, with δ_c the Kronecker delta. The resolution $D_{\phi+\delta_c}$ is nothing but the resolution obtained by changing the smoothing of c. Before stating the enhancing rules, we note that $D_{\phi+\delta_c}$ differs from D_ϕ by the merging of two circles into one or the splitting of a circle into two. The rules are then:

- if two circles are merging, then the resulting circle is labeled by the product of the labels in $\mathbb{F}_2[x]/x^2$;
- if one circle is splitting, then the resulting circles are labeled according to the coproduct of the label in $H_*(\mathbb{C}P^1; \mathbb{F}_2) \cong \mathbb{F}_2[x]/x^2$, that is
  - if the circle is 1–labeled, then there are two contributions obtained as the two ways to distribute 1 and x to the two new circles;
  - if the circle is x–labeled, then there is only one contribution obtained by labeling both new circles by x;
- all the other circles keep their labels unchanged.

Proposition 3.2 ([Kho00])**.** *The map ∂_D is 2–nilpotent.*

We set a bigrading on C_D defined, on every generator, by

$$\deg\left(D_\phi^\sigma\right) = \Big(|\phi^{-1}(1)|\,,\ |\phi^{-1}(1)| + |\sigma^{-1}(1)| - |\sigma^{-1}(x)|\Big).$$

It is easily checked that ∂_D increases the first grading by 1 and preserves the second. Forgetting the second grading, we obtain then a length $n + 1$ chain complex $\mathscr{C}_D$. By construction, $\mathscr{C}_D$ is naturally based, but for minimum distance reasons, we shall consider another set of generators, where labels are not anymore 1 and x but signs $- := 1$ and $+ := 1 + x$; a label $-$ is hence another notation for 1, whereas a $+$–labeled circle stands for the sum of the two terms for which the circle is respectively labeled by 1 and by x, all the others circles being identically labeled. These generators does not respect the second grading anymore, but ∂_D is somehow symmetrized as summarized in Figure II.3.

3.2.2 A few properties of Khovanov chain complexes

We gather now a few properties of Khovanov chain complexes that do sound relevant in a CSS code perspective.

Proposition 3.3 ([Kho00, Shu11])**.** *For any pointed link diagram D, and up to grading shift, the homology of $\mathscr{C}_D$ depends on the underlying link only, that is it is invariant under Reidemeister moves, shown in Figure II.4, and moving the marked point.*

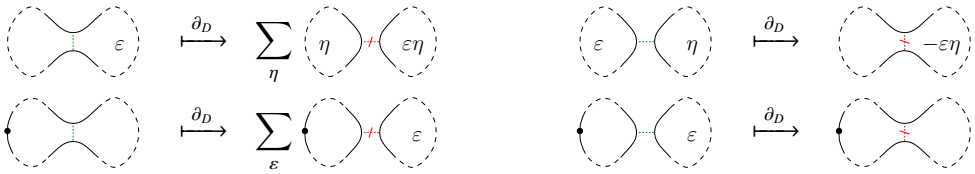


Figure II.3: Enhancing rules for ∂_D
here, ε and η are element of $\{-,+\}$ and the product is the signs multiplication

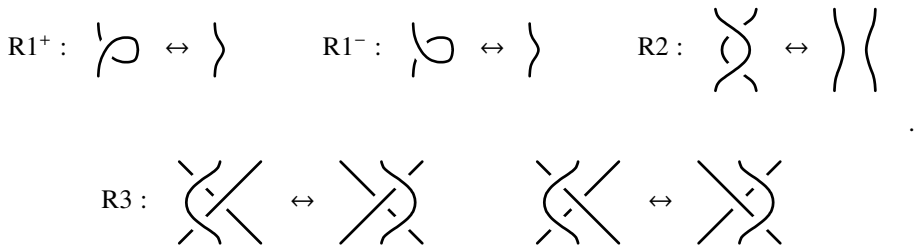


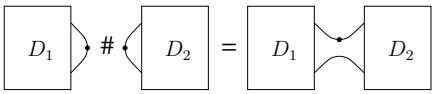
Figure II.4: Reidemeister moves

With regard to CSS codes, this proposition produces a topological way to control dimensions.

Proposition 3.4 ([Kho00])**.** *For any pointed link diagram D, and up to grading shift, $\mathscr{C}_{D!} \cong \mathscr{C}_D^*$, where $D!$ is the mirror image of D, obtained by swapping the over/under information at all crossings.*

As a CSS code address simultaneously a chain complex and its dual, this proposition ensures that both can be handled within the Khovanov homology framework.

Proposition 3.5 ([Kho00])**.** *For any two pointed link diagrams D_1 and D_2, $\mathscr{C}_{D_1\#D_2} \cong \mathscr{C}_{D_1} \otimes \mathscr{C}_{D_2}$, where $\#$ denotes the following connected sum operation:*



This proposition obviously relates the tensor product for CSS code considered in this dissertation and the connected sums of links.

Proposition 3.6 ([10, Cor. 2.11])**.** *With obvious notation for diagrams differing from a Reidemeister move, and up to the grading shift which realizes an isomorphism at the homology level, we have, for all $i \in \mathbb{Z}$*

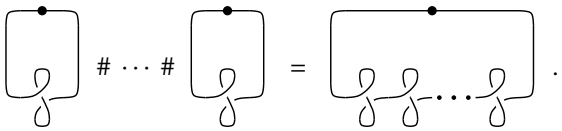
$$d_i^{\mathscr{C}_{\text{R}^+}} = 2d_i^{\mathscr{C}_{\text{R}^-}} \qquad d_i^{\mathscr{C}_{\text{R}^-}} = d_i^{\mathscr{C}_{\text{R}^-}}$$

$$\tfrac{1}{3}d_i^{\mathscr{C}_{\text{R3}}} \leq d_i^{\mathscr{C}_{\text{R3}}} \leq 2d_i^{\mathscr{C}_{\text{R3}}} \qquad \tfrac{1}{8}d_i^{\mathscr{C}_{\text{R2}}} \leq d_i^{\mathscr{C}_{\text{R2}}} \leq 8d_i^{\mathscr{C}_{\text{R2}}}$$

This proposition points out the possible relations between local moves on link diagrams and minimum distances of the associated CSS codes. At least, it offers a way to control minimum distances.

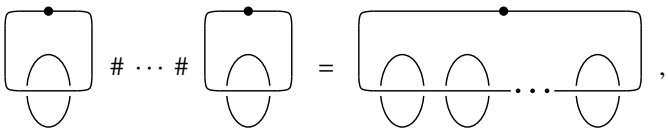
There are other properties that Khovanov homology satisfies and which are relevant for the CSS code point of view. By construction, CSS codes arising from Khovanov chain complexes have sparse matrices and families made of them shall hence have a tendancy to be LDPC. There are moreover several long exact sequences which are useful to compute homologies, but can also be used to estimate minimum distances. Finally, a reason why Khovanov homology was first believed by the author to yield valuable CSS codes is Lee spectral sequence, see [Lee05, Ras10], which converges to some very simple homology groups with generators explicitly described, in a given basis, as high–weighted elements of the initial chain complex.

Examples 3.7. A very simple example considered in [10] is the LDPC family of CSS codes arising from the following diagrams of the unknot:



The ℓ^{th} diagram of this family is obtained from the trivial diagram by performing ℓ Reidemeister R1$^+$ and ℓ Reidemeister R1$^-$ moves. It follows from Proposition 3.3 that the homology is one dimensional, from Proposition 3.4 that the associated chain complexes are symmetric and from Proposition 3.6 that the associated CSS codes have minimum distance 2^ℓ. Lengths and weights can be computed by hand, showing that the asymptotical parameters are $\left[\!\left[\frac{3^{2\ell+1}}{\sqrt{8\pi\ell}}, 1, 2^\ell, 3\ell \right]\!\right]$. This can also be seen as a consequence of Propositions 3.5 and 2.18.

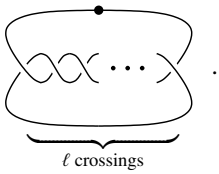
By considering the following diagrams of unlinks:



we obtain the family given in the incipit of the present section.

3.2.3 $(2, \ell)$–*torus codes*

Even if it is somewhat beyond the scope of tensor products, we end this section by a last, slightly more involved, example of Khovanov CSS codes, obtained by considering the following diagram of the $(2, \ell)$–torus link:



We denote its Khovanov chain complex by $\mathscr{C}_{(2,\ell)} := 0 \to C_0^{(2,\ell)} \to C_1^{(2,\ell)} \to \cdots \to C_\ell^{(2,\ell)} \to 0$. Using long exact sequences, all the parameters of $\mathscr{C}_{(2,\ell)}$ can be computed:

i	0	1	2	$i \in [\![3, \ell-1]\!]$	ℓ
n_i	2	ℓ	$\ell(\ell+1)$	$2^{i-1}\binom{\ell}{i}$	$2^{\ell-1}$
k_i	1	0	1	1	1
d_i	2	∞	$\frac{\ell(\ell+1)}{2}$	$\binom{\ell}{i}$	1
d_i^*	1	∞	2	2^{i-1}	$2^{\ell-1}$
w_i	2	2	3	$i+1$	0
w_i^*	0	ℓ	$2(\ell-1)$	$2(\ell-i+1)$	2

where d_i^* and w_i^* are, respectively, the minimum distance and the weight of $\mathscr{C}^*_{(2,\ell)}$ in degree i. It follows that the code $C^r_{(2,\ell)}$, defined for every $r \in \{2, \dots, \ell-1\}$ as the 3–length truncation of $\mathscr{C}_{(2,\ell)}$ around degree r, has parameters $\left[\!\left[2^{r-1}\binom{\ell}{r}, 1, \min\left(2^{r-1}, \binom{\ell}{r}\right), \max\left(r+1, 2(\ell-r+1)\right) \right]\!\right]$.

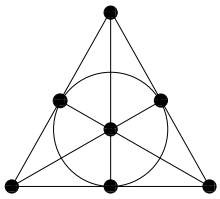


Figure II.5: The projective plane $\mathbb{P}^2(\mathbb{F}_2)$.

Among these CSS codes, low or high values for r gives poor minimum distances, but there is an efficient inbetween for which $2^{r-1} \approx \binom{\ell}{r}$. Indeed, some analysis shows that, setting $r_\ell := \mathrm{rd}\left(\alpha_0\ell - \beta_0 \ln(\ell) + \gamma_0\right)$ where $\mathrm{rd}\colon \mathbb{R} \longrightarrow \mathbb{Z}$ is any "rounding to the nearest integer" function, α_0 is the unique zero in $(0,1)$ of the function $\left(x \mapsto (2x)^x(1-x)^{1-x} - 1\right), \beta_0 := \frac{1}{2\ln\left(\frac{2\alpha_0}{1-\alpha_0}\right)}$ and $\gamma_0 := \beta_0 \ln\left(\frac{2}{\pi\alpha_0(1-\alpha_0)}\right)$, we obtain:

Proposition 3.8 ([10, Prop. 5.5])**.** *The family* $\left(C^{r_\ell}_{(2,\ell)}\right)_{\ell\geq 3}$ *is LDPC and has asymptotical parameter*

$$\left[\!\left[n_\ell, 1, > \frac{\sqrt{n_\ell}}{1,62}, O\big(\ln(n_\ell)\big)\right]\!\right],$$

with $n_\ell \sim cst.\frac{4^{\alpha_0\ell}}{\ell^{2\beta_0}}$.

3.3 Quantum finite geometry codes

Points/lines incidence structures of affine and projective spaces over finite fields are known to be a fruitful tool for error-correcting codes. It has been used to construct classical LDPC codes in [KLF01] and quantum codes in [Pos01, Aly08, Far12]. Besides points/lines incidence, we will consider here another incidence structure, the points/affine charts one, to construct short complexes. For this section, we set $q = 2^s$ for some positive integer s and denote by $\mathbb{F}_q$ the field with q elements.

3.3.1 The projective plane

The *projective plane* $\mathbb{P}^2(\mathbb{F}_q)$ is defined as the set of lines in $\mathbb{F}_q^3$ passing through the origin. A *line in* $\mathbb{P}^2(\mathbb{F}_q)$ corresponds to a plane in $\mathbb{F}_q^3$ passing through the origin, and a point of $\mathbb{P}^2(\mathbb{F}_q)$ is on a line of $\mathbb{P}^2(\mathbb{F}_q)$ if the corresponding line in $\mathbb{F}_q^3$ is contained in the corresponding plane. From now on, "points" and "lines" will refer to points and lines of $\mathbb{P}^2(\mathbb{F}_q)$. We recall now some classical facts on this finite geometry:

Proposition 3.9.

1. *The projective plane contains* $q^2 + q + 1$ *point and* $q^2 + q + 1$ *lines.*
2. *Every line contains* $q + 1$ *points and every point is contained in* $q + 1$ *lines.*
3. *Every two distinct points are contained in a unique line and every two distinct lines meet at a unique point.*

Note that each of the above statements express the principle of duality in projective planes, which swaps point and lines and reverses inclusions.

Example 3.10. For $q = 2$, the projective plane is also called *Fano plane*. It contains 7 points and 7 lines and the point/line incidence structure is usually represented by the picture given in Figure II.5 in which the 6 line segments and the circle represent the 7 lines of $\mathbb{P}^2(\mathbb{F}_2)$.

Additionally we consider *affine charts* for $\mathbb{P}^2(\mathbb{F}_q)$, which are the complements of lines. We list some properties that they satisfy:

Proposition 3.11.

1. *An affine chart is isomorphic to an affine plane over* $\mathbb{F}_q$*; in particular it contains* q^2 *elements.*

2. *Let L be a line in $\mathbb{P}^2(\mathbb{F}_q)$ and U an affine chart. Then either L is the complement of U, and hence $L \cap U = \emptyset$, or $L \cap U$ is an affine line, and hence has q elements. In particular, since q is even, the number of points of $L \cap U$ is always even.*
3. *The affine charts are in one-to-one correspondence with the lines and there are hence $q^2 + q + 1$ of them.*

3.3.2 Classical codes defined from $\mathbb{P}^2(\mathbb{F}_q)$

We construct two classical codes associated to the projective space $\mathbb{P}^2(\mathbb{F}_q)$, with length $\left|\mathbb{P}^2(\mathbb{F}_q)\right| = q^2 + q + 1$. Vectors of $\mathbb{F}^{q^2+q+1}$ can be regarded as subsets of $\mathbb{P}^2(\mathbb{F}_q)$ and we will freely speak of either vectors or subsets of $\mathbb{P}^2(\mathbb{F}_q)$. From this point of view, the canonical inner product on $\mathbb{F}^{q^2+q+1}$ can be given a geometric interpretation since, for $S, S' \subseteq \mathbb{P}^2(\mathbb{F}_q)$, $\langle S, S' \rangle = |S \cap S'| \mod 2$.

The two codes are:

- $\mathcal{C}^s_{\text{lines}}$, spanned by lines of $\mathbb{P}^2(\mathbb{F}_q)$;
- $\mathcal{C}^s_{\text{planes}}$, spanned by the affine charts of $\mathbb{P}^2(\mathbb{F}_q)$.

Warning 3.12. We want to stress the fact that, even though the projective spaces are defined over $\mathbb{F}_q$, the associated classical codes, and hence the quantum codes to follow, are defined over $\mathbb{F}_2$.

Proposition 3.13 ([Smi69])**.** *The code $\mathcal{C}^s_{\text{lines}}$ has dimension $k_{\mathcal{C}^s_{\text{lines}}} = 3^s + 1$.*

Proposition 3.14 ([2, Prop. 4.7])**.**

1. $\mathcal{C}^s_{\text{planes}} \subseteq \mathcal{C}^{s\perp}_{\text{planes}}$;
2. $\mathcal{C}^s_{\text{planes}} \subseteq \mathcal{C}^s_{\text{lines}}$;
3. $\mathcal{C}^s_{\text{planes}} \subseteq \mathcal{C}^{s\perp}_{\text{lines}}$;
4. $k_{\mathcal{C}^s_{\text{lines}}} - k_{\mathcal{C}^s_{\text{planes}}} = 1$.

Remark 3.15. Actually, $\mathcal{C}^s_{\text{planes}}$ is nothing but the *even subcode* of $\mathcal{C}^s_{\text{lines}}$ i.e. the subcodes of vectors of even weight.

3.3.3 CSS codes defined from $\mathbb{P}^2(\mathbb{F}_q)$

Definition 3.16 (Quantum finite geometry codes)**.** We define C^s_{FG} as the CSS code of length $q^2 + q + 1$ associated to the pair $\mathcal{C}^s_{\text{planes}} \subseteq \mathcal{C}^s_{\text{lines}}$.

After reduction, it corresponds to the chain complex:

$$\mathscr{C}^s_{\text{FG}} := \quad \mathbb{F}^{3^s} \hookrightarrow \mathbb{F}^{2^{2s}+2^s+1} \twoheadrightarrow \mathbb{F}^{2^{2s}+2^s-3^s} \ .$$

Indeed, point 4. of Proposition 3.14, together with Proposition 3.13, asserts that $k_{\mathcal{C}^s_{\text{planes}}} = 3^s$.

Remark 3.17. The code C^1_{FG} is nothing but the $[\![7, 1, 3]\!]$ Steane code. This fact is actually well–known, since the Steane code is known to be constructed from the Hamming code and its dual, while the Hamming code is already known to be the code $\mathcal{C}_{\text{lines}}(1)$ spanned by the lines of $\mathbb{P}^2(\mathbb{F})$.

We define now the set Ω of lines of $\mathbb{P}^2(\mathbb{F}_q)$. As consequences of Propositions 3.9, 3.11 and 3.14, we obtain:

Lemma 3.18 ([2, Lem. 4.11 and 4.12])**.**

- $\Omega \subset \mathcal{C}^s_{\text{lines}} \setminus \mathcal{C}^s_{\text{planes}}$;
- $\Omega \subset \mathcal{C}^{s\perp}_{\text{planes}} \setminus \mathcal{C}^{s\perp}_{\text{lines}}$;
- $|\Omega| = q^2 + q + 1$;
- $\text{overlap}(\Omega) = q + 1$.

Then, using simultaneously Ω for $\mathscr{C}^s_{\text{FG}}$ and $\mathscr{C}^{s*}_{\text{FG}}$ in Proposition 2.19, we obtain:

Proposition 3.19. *The family $\left(C^{s\otimes_t \ell}_{FG}\right)_{\ell \in \mathbb{N}*}$ of iterated powers of C^s_{FG} has parameters*

$$\left[\!\!\left[\sim C_s \left(4^s + 2^s + 1 + \alpha_s\right)^\ell, 1, \geq \left(\frac{4^s + 2^s + 1}{2^s + 1}\right)^\ell, \leq (4^s + 2^s + 1)\ell \right]\!\!\right]$$

with $\alpha_s := \left(2\sqrt{3}\right)^s \sqrt{1 + \left(\frac{1}{2}\right)^s - \left(\frac{3}{4}\right)^s}$ and C_s some constant depending only on s.

In particular, it is a LDPC family with constant a dimension equal to 1, but minimum distances growing faster than any "$< \frac{1}{2}$"–power of the lengths.

3.4 Quantum cyclic codes

Based on classical cyclic codes, we present now another CSS codes for which Propositions 2.18 and 2.19 can be efficiently applied. For this section, we set a positive integer n.

3.4.1 Cyclic codes

We first recall classical facts about cyclic codes. For further details we refer the interested reader to [MS77, Chapter 7]. A *cyclic code* $\mathcal{C} \subseteq \mathbb{F}_2^n$ is a code which is stable under the action of the automorphism

$$\sigma\colon \left\{ \begin{array}{ccc} \mathbb{F}^n & \longrightarrow & \mathbb{F}^n \\ (x_0, \ldots, x_{n-1}) & \longmapsto & (x_{n-1}, x_0 \ldots, x_{n-2}) \end{array} \right. .$$

Hereinafter, we identify $\mathbb{F}_2^n$ and $\mathbb{F}_2[X]/(X^n - 1)$ using the $\mathbb{F}_2$–linear isomorphism

$$\left\{ \begin{array}{ccc} \mathbb{F}_2[X]/(X^n - 1) & \xrightarrow{\sim} & \mathbb{F}_2^n \\ f = f_0 + f_1 X + \cdots + f_{n-1} X^{n-1} & \longmapsto & (f_0, \ldots, f_{n-1}) \end{array} \right.$$

and we define the weight of a polynomial as the number of its nonzero coefficents. Using this identification, the automorphism σ corresponds in $\mathbb{F}_2[X]/(X^n - 1)$ to the multiplication by X. A code $\mathcal{C} \subset \mathbb{F}_2[X]/(X^n - 1)$ is hence cyclic iff it is stable under multiplication by X, that is iff it is an ideal. But since $\mathbb{F}_2[X]$ is a principal ideal domain, the ideals of $\mathbb{F}_2[X]/(X^n - 1)$ are in one-to-one correspondence with the divisors of $X^n - 1$.

Given $h \in \mathbb{F}_2[X]$ such that $h \mid X^n - 1$, $\mathcal{C}_{\mathrm{cyc}}^h$ is defined as the code corresponding to the ideal generated by h. We shall say that h is a *generating polynomial* for $\mathcal{C}_{\mathrm{cyc}}^h$.

Proposition 3.20.

- *For every divisor h of $X^n - 1$, $k_{\mathcal{C}_{cyc}^h} = n - \deg(h)$.*
- *Generating polynomials are unique up to multiplication by an invertible element of $\mathbb{F}_2[X]/(X^n - 1)$.*
- *For every divisors h_1, h_2 of $X^n - 1$, if $h_1 | h_2$, then $\mathcal{C}_{cyc}^{h_2} \subset \mathcal{C}_{cyc}^{h_1}$.*
- *The dual of a cyclic code is cyclic. More precisely, for every divisor h of $X^n - 1$, $\mathcal{C}_{cyc}^{h\perp} = \mathcal{C}_{cyc}^{g}$, where $\bar{g} := \frac{X^n - 1}{h} \in \mathbb{F}_2[X]$ and $g = \bar{g}\left(\frac{1}{X}\right) . X^{\deg(\bar{g})}$.*

3.4.2 CSS codes defined from cyclic codes

The case $n = 2^s$ is never considered in the study of classical cyclic codes. Indeed, the polynomial $X^n - 1$ is then completely inseparable and all the constructions based on choosing divisors of $X^n - 1$ having a prescribed set of roots, such as BCH codes introduced *e.g.* in [MS77, Chapter 9]), fail. But oddly enough, this is precisely the case which will lead to CSS codes with interesting families of iterated tensor powers.

Over $\mathbb{F}_2$, $X^{2^s} - 1 = (X - 1)^{2^s}$ and the divisors of $X^n - 1$ are hence exactly the polynomials $(X - 1)^r$ with $r \in \{0, \ldots, 2^s\}$. The corresponding cyclic codes $\mathcal{C}_{\mathrm{cyc}}^{(X-1)^r}$ has dimension $n - r$ and satisfy $\mathcal{C}_{\mathrm{cyc}}^{(X-1)^r\perp} = \mathcal{C}_{\mathrm{cyc}}^{(X-1)^{n-r}}$.

Definition 3.21 (Quantum cyclic codes)**.** For every integer $r \in \{1, \ldots, n-1\}$, we define $\mathcal{C}_{\mathrm{cyc}}^{n,r}$ as the CSS code of dimension 1 associated to the pair $\mathcal{C}_{\mathrm{cyc}}^{(X-1)^r} \subseteq \mathcal{C}_{\mathrm{cyc}}(X - 1)^{r-1}$.

If $g_r : \mathbb{F}_2^{n-r} \to \mathbb{F}_2^n$ and $g_{n-r+1} : \mathbb{F}_2^{r-1} \to \mathbb{F}_2^n$ are, respectively, generating maps for $\mathcal{C}_{\mathrm{cyc}}^{(X-1)^r}$ and $\mathcal{C}_{\mathrm{cyc}}^{(X-1)^{r-1}\perp} = \mathcal{C}_{\mathrm{cyc}}^{(X-1)^{n-r+1}}$, then $\mathcal{C}_{\mathrm{cyc}}^{n,r}$ corresponds to the chain complex

$$\mathscr{C}_{\mathrm{cyc}}^{n,r} := \mathbb{F}_2^{n-r} \xhookrightarrow{g_r} \mathbb{F}_2^n \xrightarrow{g_{n-r+1}^*} \mathbb{F}_2^{r-1} .$$

Now, using Proposition 2.19 with

$$\Omega := \left\{ X^i(X-1)^{r-1} \mod (X-1)^n \;\middle|\; i \in \{0,\dots,n-1\} \right\}$$
$$\Omega' := \left\{ X^i(X-1)^{n-r} \mod (X-1)^n \;\middle|\; i \in \{0,\dots,n-1\} \right\},$$

we obtain:

Proposition 3.22 ([2, Cor. 4.17]). *For every $s \in \mathbb{N}^*$, the family $\left(C_{cyc}^{4^s,2^s\otimes_r \ell}\right)_{\ell\in\mathbb{N}^*}$ of iterated powers of $C_{cyc}^{4^2,2^s}$ has parameters*

$$\left[\!\left[\sim K_s(4^s+\beta_s)^\ell, 1, \geq 2^{s\ell}, \leq 2^s\ell \right]\!\right]$$

with $\beta_s := (2\sqrt{2})^s\left(1-\frac{1}{2^s}\right)$ and K_s some constant depending only on s.

In particular, it is a LDPC family with a constant dimension equal to 1, but minimum distances growing faster than any "$<\frac{1}{2}$"–power of the lengths.

3.5 Quantum Reed–Muller codes

Finally, we study a last family of CSS codes based on classical Reed–Muller codes, which were first introduced by L. Zhang and I. Fuss in [ZF97]. A. Steane also introduced some quantum codes based on classical Reed–Muller codes in [Ste99]; his construction is however very different since Steane's codes are stabilizer codes, but not CSS codes.

For every $r \in \mathbb{N}^*$ and $s \in \{0,\dots,r\}$, we define:

- $\mathrm{Pol}_r := \mathbb{F}_2[X_1,\dots,X_r]/(X_1^2-X_1,\dots,X_r^2-X_r)$ given with the basis $\left\{ X_I := \prod_{i\in I} X_i \;\middle|\; I \subset \{1,\dots,r\} \right\}$;
- $\mathrm{Pol}_{r,s}$ the restriction of Pol_r to elements of degree[4] at most s;
- $\phi_r : \mathrm{Pol}_r \hookrightarrow \mathbb{F}_2^{2^r}$ the evaluation map which sends a polynomial P to $\big(P(x)\big)_{x\in\mathbb{F}_2^r}$;
- $\phi_{r,s}$ the restriction of ϕ_r to $\mathrm{Pol}_{r,s}$.

The Reed–Muller code $\mathcal{C}_{\mathrm{RM}}^{r,s}$ is defined as the classical code with generating map $\phi_{r,s}$.

Proposition 3.23 ([MS77, Theorem 13.4]). *For every $r \in \mathbb{N}^*$ and $s \in \{0,,\dots,r\}$, $\mathcal{C}_{RM}^{r,s\,\perp} = \mathcal{C}_{RM}^{r,r-s-1}$.*

Definition 3.24 (Quantum Reed–Muller codes). For every $r \in \mathbb{N}^*$, we define C_{RM}^r as the CSS code of length $\binom{2r}{r}$ associated to the pair $\mathcal{C}_{\mathrm{RM}}^{2r,r-1} \subseteq \mathcal{C}_{\mathrm{RM}}^{2r,r}$.

It corresponds to the chain complex:

$$\mathscr{C}_{\mathrm{RM}}^r := \ \mathrm{Pol}_{2r,r-1} \xhookrightarrow{\ \phi_{2r,r-1}\ } \mathbb{F}^{4^r} \xrightarrow{\ \phi_{2r,r-1}^*\ } \mathrm{Pol}_{2r,r-1}\ .$$

A basis of the homology of $\mathscr{C}_{\mathrm{RM}}^r$ is given by the images through ϕ_{2r} of all $X_I \in \mathrm{Pol}_{2r}$ with $|I| = r$. Using Proposition 2.19 with

$$\Omega_{\phi_{2r}(X_I)} := \left\{ \phi_{2r}\Big(\prod_{i\in I^c}(X_i+\varepsilon_i)\Big) \;\middle|\; \forall (\varepsilon_i)_{i\in I^c} \in \mathbb{F}_2^r \right\},$$

for all $I \subset \{1,\dots,2r\}$ such that $|I| = r$, and with $I^c := \{1,\dots,2r\} \setminus I$, we obtain:

Proposition 3.25 ([2, Prop. 4.21]). *For every $r \in \mathbb{N}^*$, the family $\left(C_{RM}^{r\otimes_r \ell}\right)_{\ell\in\mathbb{N}^*}$ of iterated powers of C_{RM}^r has parameters*

$$\left[\!\left[\frac{2\left(\frac{3.4^r-\binom{2r}{r}}{2}\right)^\ell + \binom{2r}{r}^\ell}{3}, \binom{2r}{r}^\ell, 2^{r\ell}, \leq 4^r\ell \right]\!\right].$$

[4] defined by $\deg(X_I) = |I|$, with the convention that 0 has degree $-\infty$

It follows from Stirling series that, by extracting the $(\ell = r)$–diagonal subfamily, we obtain an r–indexed family with parameters

$$\left[\!\!\left[\sim \frac{\left(\frac{3}{2}\right)^{r-1} 4^{r^2}}{e^{\frac{1}{9\pi}} e^{\frac{1}{3}} \sqrt{\frac{r}{\pi}}}, \sim \frac{4^{r^2}}{e^{\frac{1}{8}} \sqrt{\pi r}^r}, 2^{r^2}, \leq 4^r r \right]\!\!\right].$$

Stricto sensu, this family is not LDPC, but the weight grows slower than any positive power of the length. Furthermore, the dimension grows faster than any "< 1"–power of the length, and the minimum distance faster than any "$< \frac{1}{2}$"–power of the length.

Perspectives

As illustrated in this dissertation, chain complexes and CSS codes are two points of view on the same combinatorial object, and all the possible contributions of each to the other have not been yet investigated.

CSS codes construction

Here and around, chain complexes have brought to light interesting CSS codes, and it is of course natural to keep on digging in this direction.

Question 1. *Can the chain complex point of view provides more new interesting examples of CSS codes ?*

In topology, CW–complexes for manifolds provide an abundant source of chain complexes. Kitaev toric codes, introduced in [Kit03], fall within this sphere. A nice feature, in this context, is that manifolds may be enhanced with geometry, and this may provide an efficient tool to deal with minimum distance. Due to its tendency to dilate distances, hyperbolic geometry is, in particular, quite promising; Freedman–Luo–Meyer codes, developped in [FLM02], take indeed advantage of it. But one difficulty, then, is to discretize the construction, in order to get a CSS code, while preserving the distances behavior. Crucial in some of the most recent breakthrough in topology, CAT(0) cube complexes is an hyperbolic geometry–related context which is more suitable for discretization, and hence for CSS codes.

Question 1.1. *May CAT(0) spaces lead to some new interesting CSS codes ?*

But CW–complexes are not the only topological source of chain complexes. Khovanov codes, presented in Section 3.2, emerged from *categorification*, a categorical and homological refoundation of classical invariants for links or manifolds. After Khovanov's seminal construction, it has been developped in many different directions: Heegaard–Floer [OS04, MOST07] homology categorifying Alexander polynomial, Khovanov–Rozansky homology [KR08a, KR08b] categorifying HOMFLY–PT polynomial, refined Khovanov homolgies for some restricted notions of links [14, 13], *etc*. The list is far from being exhaustive.

Question 1.2. *May categorification lead to some other valuable CSS codes ?*

Topology is not the only field which can provide chain complexes. Loosing maybe the geometry that may help to deal with minimum distances, but gaining on the discrete nature, homological algebra has developped tools for the study of algebra structures that may also be fruitful in a CSS codes perspective. Actually, it already is. In [Prz10], Przytycki has indeed shown that Khovanov homology of $(2, \ell)$–torus links, used in Section 3.2.3 to construct CSS codes, can be interpreted as some Hochschild homology of the $\mathbb{Z}[X]/X^2$ algebra.

Question 1.3. *May algebra lead to some new valuable CSS codes ?*

Square root barrier conjecture

In the classical setting, families of LDPC codes with a minimum distance growing linearly with the length has been known for a long time. By comparison, it is striking, in the quantum setting, that whatever the foundation of the construction is, none of the known LDPC family of CSS codes has a minimum distance growing at least as some "$> \frac{1}{2}$"–power of the length.

Question 2. *Is there a generic "square root of the length" barrier for the minimum distances of a LDPC family of CSS codes ?*

Such a barrier has already been proven for some class of CSS codes, such as euclidian codes [BPT10] or surfaces and color codes [Del13, Fet12], but it remains open in general. The very first motivation for Theorem 2.9 and its corollaries, Propositions 2.18 and 2.19, was to provide a counter-example to the square root barrier conjecture shaped as an iterated tensor powers family. Unfortunatly, Lemma 2.17 nipped this hope in the bud, not by saying that such an example does not exist, but that it could not be detected by use of the tools developped in this dissertation. Indeed, if the minimum distance of a CSS code C can be

well approached by some (N, K)–cocontrol using Corollary 2.12 , then d_C is somehow less than $\sqrt{n_C}$. In one hand, this invites to look at examples which are non suitable for Corollary 2.12; but on the other hand, this may also lead to a positive answer for the conjecture, if proving that any minimum distance can be reasonably approached by some (N, K)–cocontrol. This raises the following question:

Question 2.1. *Is there a polynomial function P such that, for every CSS code C, the chain complexes $\mathscr{C}$ and $\mathscr{C}^*$ are (N, K)–cocontrolled for some $N, K \in \mathbb{N}^*$ satisfying $d_C \leq \frac{N}{K} P(w_C)$?*

And more generally:

Question 2.2. *Is there a polynomial function P such that, for every CSS code C, $d_C \leq \sqrt{n_C P(w_C)}$?*

Decoding

Decoding is a crucial factor for error-correcting codes, and as far as the author knows, the homological machinery has not been yet exploited to this end. In that direction, spectral sequences are a powerful tool in homological algebra which starts with a filtered chain complex $\mathscr{C}$ and provides an iteratively defined sequence of chain complexes, called *pages*. The first page is the associated graded chain complex $\mathscr{C}_{gr}$, each subsequent page is the homology of the previous one, and the whole sequence converges to $H_\bullet(\mathscr{C})$. From a CSS code point of view, it provides a step-by-step approximation of the quantum errors which cannot be detected. Such a spectral sequence could be a key ingredient in some layered decoding process.

In particular, B. Everitt and P. Turner developped in [ET12] a notion of posets bundle for which they set a spectral sequence. This framework should be particularly well adapted to CSS codes admitting a local covering by hypercubes, a property which is met in several known constructions, for instance in Khovanov codes.

Question 3. *Can an efficient layered decoding process be developped, rooted on spectral sequences, and adapted to hypercubes-covered CSS codes such as Khovanov ones ?*

Return on investment for knot theory

Interactions between topology and quantum codes should not be one-way, and some code-related notions, such as minimum distance, can be pulled back and studied for topological purpose. While studying Khovanov codes, Proposition 3.6 popped up as an elementary tool to analyse minimum distances. It appeared, in particular, that modifications of the minimum distance when performing a R1 move are very well controlled. On R2 and R3 moves, the naive control is looser, but computations suggest the following:

Question 4. *Do the equalities $d_i^{\mathscr{C}_{\nearrow}} = 2d_i^{\mathscr{C}_{\shortparallel}}$ and $d_i^{\mathscr{C}_{\ll}} = d_i^{\mathscr{C}_{\nearrow}}$ hold in general or, at least, for some subfamilies of link diagrams ?*

A positive answer would lead to new invariants hidden in Khovanov homology, defined as $\frac{1}{2^{n_+}} d_i^{\mathscr{C}_D}$ where D is a link diagram with n_+ positive crossings and i is any integer in the support of $\mathscr{C}_D$. Beside the potential for distinguishing links with same Khovanov homology, this might also have some other applications, for instance to the computation of Rasmussen invariant. Indeed, based on minimum distance considerations, generic information on the first page of the Lee spectral sequence may allow to rule out from the very start some generators which are doomed to die before convergence of the sequence.

Bibliography

Personal papers

[1] B. Audoux and D. Moussard. Toward universality in degree 2 of the kricker lift of the kontsevich integral and the lescop equivariant invariant. arXiv:1710.09730, 2017.

[2] B. Audoux and A. Couvreur. On tensor products of CSS codes. arXiv:1512.07081, 2015.

[3] B. Audoux, A. Lecuona, and F. Roukema. On hyperbolic knots in S^3 with exceptional surgeries at maximal distance. arXiv:1701.01751, to appear in *Algebr. Geom. Top.*, 2017.

[4] B. Audoux, V. Bobkov, and E. Parini. On multiplicity of eigenvalues and symmetry of eigenfunctions of the p–Laplacian. arXiv:1704.03194, to appear in *Topol. Methods Nonlinear Anal.*, 2017.

[5] B. Audoux, P. Bellingeri, J.-B. Meilhan, and E. Wagner. Extensions of some classical local moves on knot diagrams. arXiv:1510.04237, to appear in *Michigan Math. J.*, 2015.

[6] B. Audoux, J.-B. Meilhan, and E. Wagner. On codimension two embeddings up to link-homotopy. *J. Topol.*, 10(4):1107–1123, 2017.

[7] B. Audoux, P. Bellingeri, J.-B. Meilhan, and E. Wagner. On usual, virtual and welded knotted objects up to homotopy. *J. Math. Soc. Japan*, 69(3):1079–1097, 2017.

[8] B. Audoux, P. Bellingeri, J.-B. Meilhan, and E. Wagner. Homotopy classification of ribbon tubes and welded string links. *Ann. Sc. Norm. Super. Pisa Cl. Sci.*, 17(1):713–761, 2017.

[9] B. Audoux. On the welded tube map. In *Knot theory and its applications*, volume 670 of *Contemp. Math.*, pages 261–284. Amer. Math. Soc., Providence, RI, 2016.

[10] B. Audoux. An application of Khovanov homology to quantum codes. *Ann. Inst. Henri Poincaré D, Comb. Phys. Interact.*, 1(2):185–223, 2014.

[11] B. Audoux. Surfaces with pulleys and Khovanov homology. *J. Knot Theory Ramifications*, 20(7):1021–1040, 2011.

[12] B. Audoux. Singular link Floer homology. *Algebr. Geom. Topol.*, 9(1):495–535, 2009.

[13] B. Audoux. Khovanov homology and star-like isotopies. *Topology Appl.*, 156(6):1054–1070, 2009.

[14] B. Audoux and T. Fiedler. A Jones polynomial for braid-like isotopies of oriented links and its categorification. *Algebr. Geom. Topol.*, 5:1535–1553, 2005.

Other papers

[Ale28] J. W. Alexander. Topological invariants of knots and links. *Trans. Amer. Math. Soc.*, 30(2):275–306, 1928.

[Aly08] S. A. Aly. A class of quantum ldpc codes constructed from finite geometries. *Proceedings of IEEE GLOBECOM 2008*, pages 1–5, 2008.

[AMT12] I. Andriyanova, D. Maurice, and J-P. Tillich. Quantum ldpc codes obtained by non-binary constructions. *Proc. IEEE Int. Symp. Info. Theo.*, pages 343–347, 2012.

[Art25] E. Artin. Zur Isotopie zweidimensionaler Flächen im $\mathbb{R}^4$. *Abh. Math. Semin. Univ. Hamb.*, 4:174–177, 1925.

[Art47] E. Artin. Theory of braids. *Ann. Math.*, 48(1):174–177, 1947.

[Bar95] D. Bar-Natan. On the Vassiliev knot invariants. *Topology*, 34(2):423–472, 1995.

[BD16] D. Bar-Natan and Z. Dancso. Finite-type invariants of w-knotted objects. I: *w*-knots and the Alexander polynomial. *Algebr. Geom. Topol.*, 16(2):1063–1133, 2016.

[BH13a] S. Bravyi and M. B. Hastings. Homological product codes. arXiv:1311.0885, 2013.

[BH13b] T. E. Brendle and A. Hatcher. Configuration spaces of rings and wickets. *Comment. Math. Helv.*, 88(1):131–162, 2013.

[BH14] S. Bravyi and M. B. Hastings. Homological product codes. In *Proceedings of the 46th annual ACM symposium on theory of computing, STOC '14. New York, NY, USA, May 31– June 04, 2014*, pages 273–282. ACM, 2014.

[BL93] J. S. Birman and X-S. Lin. Knot polynomials and Vassiliev's invariants. *Invent. Math.*, 111(2):225–270, 1993.

[BMD07] H. Bombin and M. Martin-Delgado. Homological error correction: classical and quantum codes. *J. Math. Phys.*, 48(5):052105, 2007.

[BMv78] E. B. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Inf. Theory*, 24:384–386, 1978.

[BPT10] S. Bravyi, D. Poulin, and B. Terhal. Tradeoffs for reliable quantum information storage in 2d systems. *Phys. Rev. Lett.*, 104:050503, 2010.

[BT99] A. Bartels and P. Teichner. All two dimensions links are null homotopic. *Geom. Topol.*, 3:235–252, 1999.

[CDZ13] A. Couvreur, N. Delfosse, and G. Zémor. A construction of quantum LDPC codes from Cayley graphs. *IEEE Trans. Inform. Theory*, 59(9):6087–6098, 2013.

[CKS04] J. S. Carter, S. Kamada, and M. Saito. *Surfaces in 4-space*, volume 142 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2004. Low-Dimensional Topology, III.

[COT07] T. Camara, H. Ollivier, and J-P. Tillich. A class of quantum LDPC codes: constructions and performances under iterative decoding. *Proc. IEEE Int. Symp. Info. Theo.*, Nice:811–815, 2007.

[CS96] R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098:1098–1105, 1996.

[CS98] J. S. Carter and M. Saito. *Knotted surfaces and their diagrams*, volume 55 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1998.

[CST12] J. Conant, R. Schneiderman, and P. Teichner. Whitney tower concordance of classical links. *Geom. Topol.*, 16(3):1419–1479, 2012.

[Del12] N. Delfosse. *Constructions et performances de codes LDPC quantiques*. PhD thesis, University of Bordeaux, 2012.

[Del13] N. Delfosse. Tradeoffs for reliable quantum information storage in surface codes and color codes. In *2013 IEEE International Symposium on Information Theory*, pages 917–921, 2013.

[Djo08] I. B. Djordjevic. Quantum LDPC codes from incomplete block designs. *IEEE Communication Letters*, 12(5):389–391, 2008.

[ET12] B. Everitt and P. Turner. Bundles of coloured posets and a Leray–Serre spectral sequence for Khovanov homology. *Trans. Amer. Math. Soc.*, 364(6):3137–3158, 2012.

[Far12] J. Farinholt. Quantum LDPC codes constructed from point-line subsets of the finite projective plane. ArXiv:1207.0732, 2012.

[Fet12] E. Fetaya. Bounding the distance of quantum surface codes. *J. Math. Phys.*, 53(6):062202, 2012.

[FH14] M. H. Freedman and M. B. Hastings. Quantum systems on non-k-hyperfinite complexes: A generalization of classical statistical mechanics on expander graphs. *Quantum Inf. Comput.*, 14(1–2):144–180, 2014.

[Fie01] T. Fiedler. *Gauss diagram invariants for knots and links*, volume 532 of *Mathematics and its Applications*. Kluwer Academic Publishers, 2001.

[FLM02] M. H. Freedman, F. Luo, and D. A. Meyer. Z_2-systolic freedom and quantum codes. In *Mathematics of quantum computation*, Comput. Math. Ser., pages 287–320. Chapman & Hall/CRC, Boca Raton, FL, 2002.

[FM66] R. H. Fox and J. W. Milnor. Singularities of 2–spheres in 4–space and cobordism of knots. *Osaka J. Math.*, 3:257–267, 1966.

[FM01] M. H. Freedman and D. A. Meyer. Projective plane and planar quantum codes. *Found. Comput. Math.*, 1(3):325–332, 2001.

[FQ90] M. H. Freedman and F. S. Quinn. *Topology of 4-manifolds*. Princeton, NJ: Princeton University Press, 1990.

[Gal62] R. G. Gallager. *Low density parity check codes*. PhD thesis, Massachussetts Institute of Technology, 1962.

[GFL08] J. Garcia-Frias and K. Liu. Design of near-optimum quantum error-correcting codes based on generator and parity-check matrices of ldgm codes. *Proceedings of CISS*, Princeton:562–567, 2008.

[Gou94] M. Goussarov. On n-equivalence of knots and invariants of finite degree. In *Topology of manifolds and varieties. Transl. ed. by A. B. Sossinsky*, pages 173–192. Providence, RI: American Mathematical Society, 1994.

[GPV00] M. Goussarov, M. Polyak, and O. Viro. Finite-type invariants of classical and virtual knots. *Topology*, 39(5):1045–1068, 2000.

[Hag08] M. Hagiwara. Quantum error-correcting codes. In *Mathematical aspects of quantum computing 2007. Papers based on the presentations at the summer school, Osaka, Japan, August 27–29, 2007.*, pages 181–212. Hackensack, NJ: World Scientific, 2008.

[Hem76] J. Hempel. 3-*Manifolds*. Princeton University Press, Princeton, N. J.; University of Tokyo Press, Tokyo, 1976. Ann. of Math. Studies, No. 86.

[Hir59] M. W. Hirsch. Immersions of manifolds. *Trans. Am. Math. Soc.*, 93:242–276, 1959.

[HL90] N. Habegger and X-S. Lin. The classification of links up to link-homotopy. *J. Amer. Math. Soc.*, 3:389–419, 1990.

[HL98] N. Habegger and X-S. Lin. On link concordance and Milnor's $\overline{\mu}$ invariants. *Bull. London Math. Soc.*, 30(4):419–428, 1998.

[HM12] K. Habiro and G. Massuyeau. From mapping class groups to monoids of homology cobordisms: a survey. In *Handbook of Teichmüller theory. Volume III*, pages 465–529. Zürich: European Mathematical Society (EMS), 2012.

[HS97] P. J. Hilton and U. Stammbach. *A course in homological algebra*, volume 4 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[IM07] L. Ioffe and M. Mézard. Asymmetric quantum error-correcting codes. *Phys. Rev. A (3)*, 75(3):032345, 4, 2007.

[Jon87] V. Jones. Hecke algebra representations of braid groups and link polynomials. *Ann. Math.*, 126(2):335–388, 1987.

[Kam99] S. Kamada. Unknotting immersed surface-links and singular 2-dimensional braids by 1-handle surgeries. *Osaka J. Math.*, 36(1):33–49, 1999.

[Ker65] M. A. Kervaire. Les nœuds de dimensions supérieures. *Bull. Soc. Math. Fr.*, 93:225–271, 1965.

[Kho00] M. Khovanov. A categorification of the Jones polynomial. *Duke Math. J.*, 101(3):359–426, 2000.

[Kho03] M. Khovanov. Patterns in knot cohomology I. *Experiment. Math.*, 12(3):365–374, 2003.

[Kit03] A. Y. Kitaev. Fault-tolerant quantum computation by anyons. *Ann. Physics*, 303(1):2–30, 2003.

[KLF01] Y. Kou, S. Lin, and M. P. C. Fossorier. Low-density parity-check codes based on finite geometries: a rediscovery and new results. *IEEE Trans. Inform. Theory*, 47(7):2711–2736, 2001.

[KM61] M. A. Kervaire and J. W. Milnor. On 2-spheres in 4-manifolds. *Proc. Natl. Acad. Sci. USA*, 47:1651–1657, 1961.

[Kon93] M. Kontsevich. Vassiliev's knot invariants. In *I. M. Gelfand seminar. Part 2: Papers of the Gelfand seminar in functional analysis held at Moscow University, Russia, September 1993*, pages 137–150. Providence, RI: American Mathematical Society, 1993.

[KR08a] M. Khovanov and L. Rozansky. Matrix factorizations and link homology. *Fund. Math.*, 199:1–91, 2008.

[KR08b] M. Khovanov and L. Rozansky. Matrix factorizations and link homology II. *Geom. Topol.*, 12:1387–1425, 2008.

[Kre14] D. A. Krebes. Units of the string link monoids. In *Knots in Poland III, Part III. Proceedings of the 3rd conference, Stefan Banach International Mathematical Center, Warsaw, Poland, July 18–25, 2010 and Będlewo, Poland, July 25 – August 4, 2010*, pages 233–240. Warszawa: Polish Academy of Sciences, Institute of Mathematics, 2014.

[Kup03] G. Kuperberg. What is a virtual link ? *Algebr. Geom. Topol.*, 3:587–591, 2003.

[Lan02] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Lee05] E. S. Lee. An endomorphism of the Khovanov invariant. *Adv. Math.*, 197(2):554–586, 2005.

[Mat87] S. V. Matveev. Generalized surgeries of three-dimensional manifolds and representations of homology spheres. *Mat. Zametki*, 42(2):268–278, 345, 1987.

[Mil54] J. Milnor. Link groups. *Ann. of Math. (2)*, 59:177–195, 1954.

[MKS04] W. Magnus, A. Karrass, and D. Solitar. *Combinatorial group theory. Presentations of groups in terms of generators and relations. Reprint of the 1976 second edition.* Mineola, NY: Dover Publications, reprint of the 1976 second edition edition, 2004.

[ML95] S. Mac Lane. *Homology*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the 1975 edition.

[MMM04] D. J. C MacKay, G. Mitchison, and P. L McFadden. Sparse-graph codes for quantum error correction. *IEEE Trans. Inf. Theory*, 50(10):2315–2330, 2004.

[MN89] H. Murakami and Y. Nakanishi. On a certain move generating link-homology. *Math. Ann.*, 284(1):75–89, 1989.

[MOST07] C. Manolescu, P. Ozsváth, Z. Szabó, and D. Thurston. On combinatorial link floer homology. *Geom. Topol.*, 11(4):2339–2412, 2007.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes I*. North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[MY17] J-B. Meilhan and A. Yasuhara. Arrow calculus for welded and classical links. arXiv:1703.04658, 2017.

[NC10] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press. xxxi, Cambridge, 10th anniversary editions edition, 2010.

[OS04] P. Ozsváth and Z. Szabó. Holomorphic disks and knot invariants. *Adv. Math.*, 186(1):58–116, 2004.

[PC08] D. Poulin and Y. Chung. On the iterative decoding of sparse quantum codes. *Quantum Inf. Comput.*, 8(10):987–1000, 2008.

[Pos01] M. Postol. A proposed quantum low density parity check code. arXiv:quant-ph/0108131, 2001.

[Pre] J. Preskill. Quantum information and computation. `http://www.theory.caltech.edu/people/preskill/ph229/`.

[Prz10] J. Przytycki. When the theories meet: Khovanov homology as Hochschild homology of links. *Quantum Topol.*, 1(2):93–109, 2010.

[PV94] Michael Polyak and Oleg Viro. Gauss diagram formulas for Vassiliev invariants. *Internat. Math. Res. Notices*, 11:445ff., approx. 8 pp. (electronic), 1994.

[Ras03] J. Rasmussen. *Floer homology and knot complements*. PhD thesis, Harvard University, 2003.

[Ras10] J. Rasmussen. Khovanov homology and the slice genus. *Invent. Math.*, 182(2):419–447, 2010.

[Rei27] K. Reidemeister. Elementare Begründung der Knotentheorie. *Abh. Math. Sem. Univ. Hamburg*, 5(1):24–32, 1927.

[Ros98a] D. Roseman. Reidemeister-type moves for surfaces in four-dimensional space. In *Knot theory. Proceedings of the mini-semester, Warsaw, Poland, 1995*, pages 347–380. Warszawa: Polish Academy of Sciences, Institute of Mathematics, 1998.

[Ros98b] W. Rosicki. Some simple invariants of the position of a surface in $\mathbb{R}^4$. *Bulletin of the Polish Academy of Sciences. Mathematics*, Vol. 46, no 4:335–344, 1998.

[RSU01] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke. Design of capacity-approaching irregular low-density parity-check codes. *IEEE Trans. Inform. Theory*, 47:619–637, 2001.

[RT90] N. Y. Reshetikhin and V. G. Turaev. Ribbon graphs and their invariants derived from quantum groups. *Commun. Math. Phys.*, 127(1):1–26, 1990.

[Sat00] S. Satoh. Virtual knot presentation of ribbon torus-knots. *J. Knot Theory Ramifications*, 9(4):531–542, 2000.

[Shu11] A. N. Shumakovitch. Patterns in odd Khovanov homology. *J. Knot Theory Ramifications*, 20(1):203–222, 2011.

[Smi69] K. J. C. Smith. On the p–rank of the incidence matrix of points and hyperplanes in a finite projective geometry. *J. Combin. Theory*, 7(2):122–129, 1969.

[SRK08] K. P. Sarvepalli, M. Rötteler, and A. Klappenecker. Asymmetric quantum ldpc codes. *Proc. IEEE Int. Symp. Info. Theo.*, Toronto:305–309, 2008.

[Sta65] J. Stallings. Homology and central series of groups. *J. Algebra*, 2:170–181, 1965.

[Ste96] A. Steane. Multiple particle interference and quantum error correction. *Proc. Roy. Soc. Lond. A*, 452:2551:2551–2577, 1996.

[Ste99] A. Steane. Quantum reed-muller codes. *IEEE Trans. Inform. Theory*, 45(5):1701–1703, 1999.

[Suz76] S. Suzuki. Knotting problems of 2-spheres in 4-sphere. *Math. Sem. Notes Kobe Univ.*, 4(3):241–371, 1976.

[Tai84] P. G. Tait. On knots III. *Trans. Roy. Soc. Edinburgh*, 32:493–506, 1884.

[Tur17] P. Turner. Five lectures on Khovanov homology. *J. Knot Theory Ramifications*, 26(3):41, 2017.

[TZ14] J-P. Tillich and G. Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength. *IEEE Trans. Inform. Theory*, 60(2):1193–1202, 2014.

[Vas90] V. A. Vassiliev. Cohomology of knot spaces. Theory of singularities and its applications, Adv. Sov. Math. 1, 23-69, 1990.

[Vir04] O. Viro. Khovanov homology, its definitions and ramifications. *Fund. Math.*, 184:317–342, 2004.

[Wei94] C. A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.

[Win09] B. Winter. The classification of spun torus knots. *J. Knot Theory Ramifications*, 18(9):1287–1298, 2009.

[Wit94] E. Witten. Quantum field theory and the Jones polynomial. In *Braid group, knot theory and statistical mechanics II*, pages 361–451. London: World Scientific, 1994.

[Yaj62] T. Yajima. On the fundamental groups of knotted 2-manifolds in the 4-space. *J. Math. Osaka City Univ.*, 13:63–71, 1962.

[Yan69a] T. Yanagawa. On ribbon 2-knot: The 3-manifold bounded by the 2-knots. *Osaka J. Math.*, 6:447–464, 1969.

[Yan69b] T. Yanagawa. On ribbon 2-knots II: The second homotopy group of the complementary domain. *Osaka J. Math.*, 6:465–473, 1969.

[Yan70] T. Yanagawa. On Ribbon 2-knots III: On the unknotting Ribbon 2-knots in S^4. *Osaka J. Math.*, 7:165–172, 1970.

[Yur08] E. Yurasovskaya. *Homotopy String Links Over Surfaces*. PhD thesis, University of British Columbia, 2008.

[Zém09] Gilles Zémor. On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction. In *Coding and cryptology*, volume 5557 of *Lecture Notes in Comput. Sci.*, pages 259–273. Springer, Berlin, 2009.

[ZF97] Lin Zhang and Ian Fuss. Quantum reed-muller codes. ArXiv:quant-ph/9703045, 1997.